Sécurité des plateformes Apple

Mai 2021

Table des matières

Introduction à la sécurité des plateformes Apple

Apple place la sécurité au cœur de ses plateformes. Forte de son expérience de la création du système d'exploitation mobile le plus avancé au monde, Apple conçoit des architectures de sécurité qui répondent aux exigences uniques des appareils mobiles, des montres, des ordinateurs de bureau et des accessoires de domotique.

Chaque appareil Apple combine des *logiciels*, du *matériel* et des *services* qui travaillent en synergie pour assurer une protection optimale et une expérience utilisateur transparente, toujours dans l'objectif de protéger les renseignements personnels. Par exemple, la puce et le matériel de sécurité conçus par Apple propulsent des fonctionnalités de sécurité essentielles. Par ailleurs, les protections logicielles veillent à sécuriser le système d'exploitation et les apps tierces. Enfin, les services fournissent un mécanisme pour des mises à jour logicielles sécuritaires et opportunes, alimentent un écosystème d'apps protégé et facilitent les communications et les paiements sécurisés. Par conséquent, les systèmes d'exploitation d'Apple contribuent à protéger l'appareil et ses données, mais également l'écosystème en entier, y compris tout ce que l'utilisateur fait localement, sur les réseaux et par l'intermédiaire des principaux services Internet.

Nous concevons nos appareils pour qu'ils soient non seulement simples, intuitifs et performants, mais aussi sécuritaires. Les principales fonctionnalités de sécurité, comme le chiffrement matériel des appareils, ne sont pas désactivables par accident. D'autres fonctionnalités, comme Touch ID et Face ID, améliorent l'expérience de l'utilisateur : la protection de l'appareil est simple et intuitive. De plus, puisque bon nombre de ces fonctionnalités sont activées par défaut, les utilisateurs et les services des TI n'ont pas à réaliser de configurations poussées.

Le présent document explique en détail les technologies et fonctionnalités de sécurité des plateformes Apple. C'est un outil qui aidera les organisations à combiner ces technologies et fonctionnalités à leurs propres politiques et procédures pour répondre à leurs besoins en matière de sécurité.

Le contenu s'articule autour des thèmes suivants :

- **Sécurité matérielle et biométrie :** la puce et le matériel qui forment la base de la sécurité sur les appareils Apple, y compris le Secure Enclave, un moteur de chiffrement AES dédié, Touch ID et Face ID
- **Sécurité du système :** les fonctions matérielles et logicielles intégrées qui permettent le démarrage, la mise à jour et le fonctionnement sécurisés des systèmes d'exploitation Apple

- **Chiffrement et protection des données :** l'architecture et la conception qui protègent les données de l'utilisateur en cas de perte ou de vol de l'appareil, ou en cas de tentative d'utilisation ou de modification de celui-ci par une personne ou un processus non autorisés
- **Sécurité des apps :** les logiciels et services qui offrent un écosystème d'apps sécurisé et qui permettent aux apps de s'exécuter en toute sécurité, sans compromettre l'intégrité de la plateforme
- **Sécurité des services :** les services d'Apple relatifs à l'identification, à la gestion des mots de passe, aux paiements, aux communications et à la localisation des appareils perdus
- **Sécurité des réseaux :** les protocoles réseau standards qui assurent une authentification sécurisée et le chiffrement des données en transit
- **Sécurité de la trousse de développement :** les cadres d'application sous forme de trousses qui visent la gestion sécurisée et privée du domicile et de la santé, ainsi que l'extension des fonctionnalités des appareils et des services Apple aux apps tierces
- **Gestion sécurisée des appareils :** les méthodes qui autorisent la gestion des appareils Apple, contribuent à empêcher l'usage non autorisé et permettent d'effacer les données à distance en cas de perte ou de vol

Engagement en matière de sécurité

Apple s'engage à préserver la vie privée de ses clients grâce à des technologies de pointe en matière de sécurité et de confidentialité ainsi qu'à des méthodes exhaustives visant à protéger renseignements personnels et données d'entreprise. Apple récompense le travail des chercheurs qui découvrent des failles en offrant une prime de sécurité. Pour en savoir plus sur le programme et les catégories de primes, visitez le site https://developer.apple.com/security-bounty/ (en anglais seulement).

Notre équipe chargée de la sécurité assure le soutien pour tous les produits Apple. Elle fournit des services de vérification et de test de sécurité, autant pendant la conception des produits qu'après leur mise en marché. L'équipe Apple offre également de la formation et des outils de sécurité, et surveille de près les menaces et les problèmes de sécurité signalés. Apple fait partie du forum FIRST (Forum of Incident Response and Security Teams), qui rassemble des équipes de sécurité et d'intervention en cas d'incident.

Apple continue de repousser les limites du possible en matière de sécurité et de confidentialité. Cette année, tous les appareils Apple des gammes Apple Watch, iPhone, iPad et maintenant Mac qui sont dotés d'un système sur une puce utilisent une puce spéciale qui assure à la fois la sécurité et la puissance de calcul. La puce Apple forme la base du démarrage sécurisé, de Touch ID, de Face ID, de la protection des données, ainsi que des fonctionnalités d'intégrité système jamais vues sur Mac, y compris la protection de l'intégrité du noyau, les codes d'authentification des pointeurs et les restrictions d'autorisation rapide. Ces fonctionnalités d'intégrité aident à prévenir les techniques d'attaque courantes qui ciblent la mémoire, manipulent les instructions et utilisent JavaScript sur le Web. Et si le code de l'assaillant parvient malgré tout à s'exécuter, elles feront front commun pour limiter les dégâts.

Pour tirer parti de l'étendue des fonctionnalités de sécurité qui sont intégrées à nos plateformes, les organisations devraient revoir leurs politiques en matière de TI et de sécurité pour s'assurer qu'elles exploitent au mieux les couches de technologies de sécurité offertes.

Pour en savoir plus sur le signalement de problèmes à Apple et l'abonnement aux notifications sur la sécurité, consultez la page Signaler une vulnérabilité affectant la sécurité ou la confidentialité.

Chez Apple, nous croyons que le respect de la vie privée est un droit fondamental. Nous avons intégré à nos produits de nombreuses commandes et options qui permettent aux utilisateurs de décider comment et quand les apps utilisent leurs données, et quelles données sont utilisées. Pour en savoir plus sur Apple et la protection des renseignements personnels, les réglages de confidentialité intégrés aux appareils et la politique de confidentialité d'Apple, rendez-vous sur http://www.apple.com/ca/fr/privacy/**.**

Remarque : Sauf indication contraire, le présent document porte sur les systèmes d'exploitation suivants : iOS 14.5, iPadOS 14.5, macOS 11.3, tvOS 14.5 et watchOS 7.4.

Sécurité matérielle et biométrie

Aperçu de la sécurité matérielle

La sécurité des logiciels doit reposer sur des fonctionnalités intégrées au matériel. C'est pourquoi les appareils Apple, qui exécutent iOS, iPadOS, macOS, tvOS et watchOS, comprennent des fonctionnalités de sécurité à même leurs composants. Ces remparts incluent un processeur central avec capacités sur mesure assurant la protection du système et une puce dédiée à la sécurité. Le matériel axé sur la sécurité obéit à un principe : prendre en charge des fonctionnalités limitées et discrètes afin de réduire la surface d'attaque. Parmi ces composants, on trouve une mémoire morte d'amorçage, qui constitue une base matérielle sécurisée pour le démarrage, des moteurs AES dédiés, qui permettent un chiffrement et un déchiffrement sûrs et efficaces, et un coprocesseur Secure Enclave. Le *Secure Enclave* est un système sur une puce présent sur tous les modèles récents d'iPhone, iPad, Apple Watch, Apple TV et HomePod ainsi que sur les Mac à puce Apple et à puce T2 Security. Il est conçu selon les mêmes principes que les autres systèmes sur une puce et contient une mémoire morte d'amorçage et un moteur AES propres. Il fournit aussi la base sur laquelle s'appuient la création et le stockage sécurisés des clés pour le chiffrement des données au repos, et protège et évalue les données biométriques de Touch ID et Face ID.

Le chiffrement des supports de données doit être rapide et efficace. Il ne doit toutefois pas exposer les données (ou le *matériel de chiffrement*) qu'il utilise pour établir un contexte de chiffrement cryptographique. Le moteur AES physique règle ce problème en assurant un chiffrement et un déchiffrement rapides, *au fil de l'écriture ou de la lecture des fichiers*. Un canal spécial partant du Secure Enclave transmet le matériel de chiffrement nécessaire au moteur AES sans exposer l'information au processeur d'application (ou processeur central) ni au système d'exploitation général. Cela contribue à garantir que FileVault et la technologie de protection des données d'Apple peuvent protéger les fichiers des utilisateurs sans révéler les clés de chiffrement longue durée.

Le démarrage sécurisé empêche la modification des couches logicielles inférieures tout en veillant à ce que seuls les logiciels système vérifiés par Apple s'ouvrent quand l'utilisateur allume son appareil. Il prend sa source dans un code immuable appelé « mémoire morte d'amorçage », qui est défini pendant la fabrication du système sur une puce d'Apple et qui fait office de *base matérielle sécurisée*. Sur les ordinateurs Mac dotés d'une puce T2, la fiabilité du démarrage sécurisé commence par la puce elle-même. (La puce T2 et le Secure Enclave exécutent aussi chacun un processus de démarrage sécurisé à l'aide d'une mémoire morte d'amorçage distincte, mécanisme identique à celui des puces M1 et de série A.)

Le Secure Enclave traite par ailleurs les données d'empreinte digitale et de reconnaissance faciale recueillies par les capteurs de Touch ID et Face ID. Cela garantit une authentification sécurisée tout en assurant l'intégrité et la confidentialité des données biométriques. Les utilisateurs profitent ainsi de la sécurité accrue des codes et mots de passe longs et complexes, en plus de la commodité d'une authentification rapide pour valider les accès et les achats.

Sécurité du système sur une puce d'Apple

Les puces conçues par Apple forment une architecture uniforme sur l'ensemble des produits Apple; aujourd'hui, elles propulsent aussi bien les ordinateurs Mac que les appareils iPhone, iPad, Apple TV et Apple Watch. Depuis plus de 10 ans, l'équipe d'exception chargée de la conception des processeurs Apple produit et perfectionne les systèmes sur une puce d'Apple. Le résultat est une architecture qui s'adapte à tous les appareils et qui est en avance sur l'industrie sur le plan de la sécurité. Seule une entreprise qui conçoit à la fois les puces et les logiciels de ses appareils est en mesure de proposer une fondation commune pour les fonctionnalités de sécurité.

Les puces Apple sont précisément conçues et fabriquées pour prendre en charge les fonctionnalités de sécurité suivantes.

Fonctionnalité	A10	A11, S3	A12, S4	A13, S5	A14, S6	M1
Protection de l'intégrité du noyau	✓	✓	✓	✓	✓	✓
Restrictions d'autorisation rapide		✓	✓	✓	✓	✓
Protection de l'intégrité du coprocesseur système			✓	✓	✓	✓
Codes			✓	✓	✓	✓
Couche de protection de page		✓	✓	✓	✓	Voir la remarque ci-dessous.

Remarque : La couche de protection de page (PPL) exige que la plateforme exécute *uniquement* du code signé et de confiance. Ce modèle de sécurité ne s'applique pas à macOS.

Les puces conçues par Apple offrent aussi les fonctionnalités de protection des données particulières suivantes.

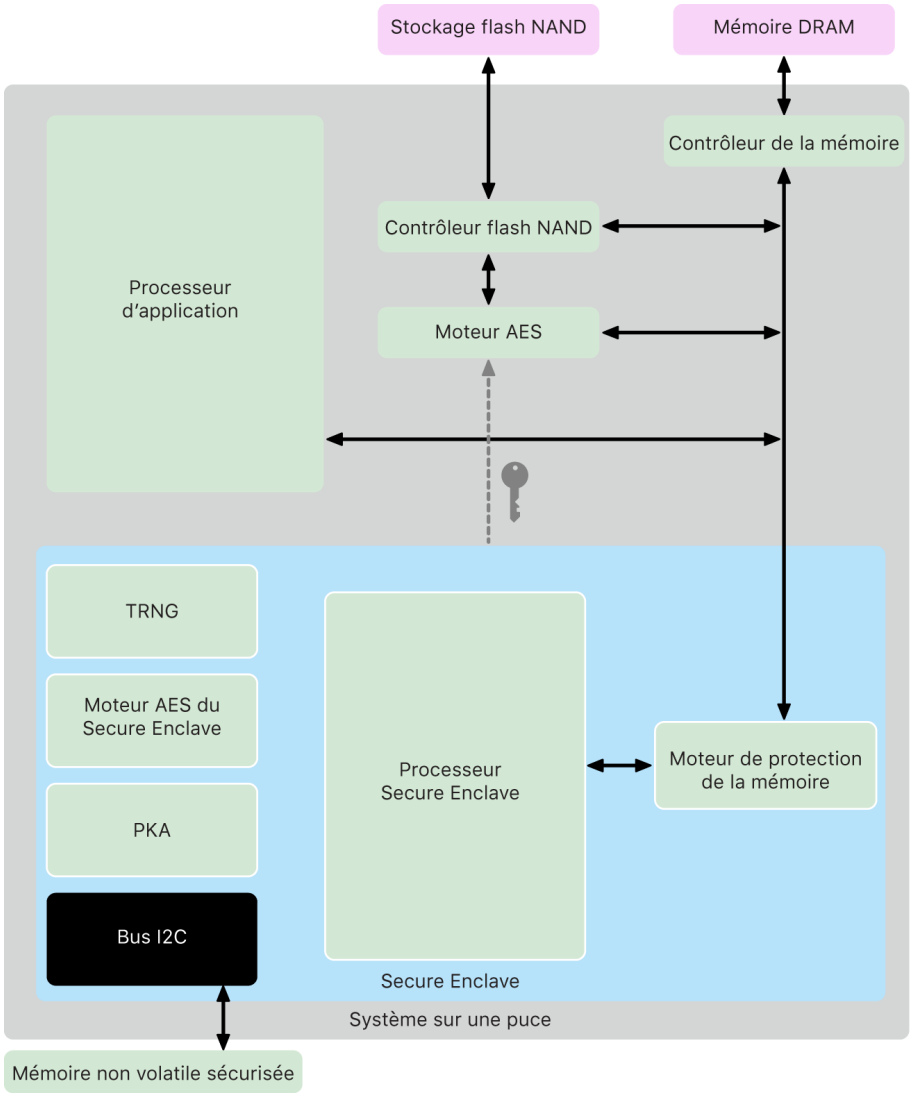
Fonctionnalité	A10	A11, S3	A12, S4	A13, S5	A14, M1, S6
Protection scellée des clés (SKP)	✓	✓	✓	✓	✓

Fonctionnalité	A10	A11, S3	A12, S4	A13, S5	A14, M1, S6
recoveryOS : toutes les classes de protection des données sont protégées.	✓	✓	✓	✓	✓
Autres démarrages du mode DFU, Diagnostic Apple et mises à jour logicielles : les données des classes A, B et C sont protégées			✓	✓	✓

Secure Enclave

Aperçu

Le Secure Enclave est un sous-système sécurisé dédié intégré aux systèmes sur une puce d'Apple. Le Secure Enclave est isolé du processeur principal pour fournir une couche supplémentaire de sécurité. Il est conçu pour sécuriser les données sensibles de l'utilisateur, et ce, même lorsque le noyau du processeur d'application est compromis. Il suit les mêmes principes que le système sur une puce : une mémoire morte d'amorçage pour établir une base matérielle sécurisée, un moteur AES assurant des opérations de chiffrement sûres et efficaces et une mémoire protégée. Bien que le Secure Enclave ne comporte pas d'espace de stockage, il dispose d'un mécanisme pour stocker les informations de façon sécuritaire sur un dispositif de stockage rattaché qui est indépendant du stockage flash NAND utilisé par le processeur d'application et le système d'exploitation.



Les composants du Secure Enclave.

Le Secure Enclave est une fonctionnalité matérielle qui est intégrée à la plupart des modèles d'iPhone, d'iPad, de Mac, d'Apple TV, d'Apple Watch et de HomePod, à savoir :

- iPhone 5s et modèles plus récents;
- iPad Air et modèles plus récents;
- les ordinateurs MacBook Pro avec Touch Bar (2016 et 2017) équipés de la puce T1 d'Apple;
- les ordinateurs Mac avec processeur Intel équipés de la puce T2 Security d'Apple;
- les ordinateurs Mac avec puce Apple;
- Apple TV HD et modèles plus récents;
- Apple Watch Series 1 et modèles plus récents;
- HomePod et HomePod mini

Processeur Secure Enclave

Le processeur Secure Enclave est la principale source de puissance de calcul du Secure Enclave. Pour assurer une isolation maximale, le processeur Secure Enclave est à l'usage exclusif du Secure Enclave. Cela permet de prévenir les attaques par canal auxiliaire, qui dépendent de logiciels malveillants partageant le même cœur d'exécution que le logiciel ciblé.

Le processeur Secure Enclave exécute une version adaptée du micronoyau L4. Il est conçu pour fonctionner efficacement à une fréquence d'horloge inférieure, ce qui le prémunit contre les attaques temporelles et les attaques par analyse de consommation. À partir des systèmes sur une puce A11 et S4, le processeur Secure Enclave comprend un moteur de protection de la mémoire, une mémoire chiffrée dotée de capacités antirejeu, le démarrage sécurisé, un générateur de nombres aléatoires dédié et un moteur AES propre.

Moteur de protection de la mémoire

Le Secure Enclave fonctionne à partir d'une zone dédiée de la mémoire vive dynamique (DRAM) de l'appareil. Plusieurs couches de protection isolent la mémoire protégée du Secure Enclave du processeur d'application.

Lorsque l'appareil démarre, la mémoire morte d'amorçage du Secure Enclave génère une clé de protection de la mémoire éphémère destinée au moteur de protection de la mémoire. Chaque fois que le Secure Enclave écrit dans sa zone de mémoire dédiée, le moteur de protection de la mémoire chiffre le bloc de mémoire au moyen de l'algorithme AES en mode XEX (xor-encrypt-xor) dans le Mac, et calcule une balise d'authentification CMAC (Cipher-based Message Authentication Code, code d'authentification de message basé sur le chiffrement) pour la mémoire. Le moteur de protection de la mémoire stocke la balise d'authentification avec la mémoire chiffrée. Lorsque le Secure Enclave lit la mémoire, le moteur de protection de la mémoire vérifie la balise d'authentification. Si la balise d'authentification concorde, le moteur de protection de la mémoire déchiffre le bloc de mémoire. Dans le cas contraire, le moteur de protection de la mémoire signale une erreur au Secure Enclave. À la suite d'une erreur d'authentification, le Secure Enclave n'accepte plus aucune demande jusqu'au redémarrage du système.

À partir des systèmes sur une puce A11 et S4 d'Apple, le moteur de protection de la mémoire comporte un dispositif antirejeu qui protège la mémoire du Secure Enclave. Afin de contribuer à prévenir toute retransmission de données essentielles, le moteur de protection de la mémoire stocke un nonce destiné au bloc de mémoire pour accompagner la balise d'authentification. Le nonce sert à perfectionner la balise d'authentification CMAC. Les nonces de tous les blocs de mémoire sont protégés au moyen d'une arborescence d'intégrité rattachée à la mémoire vive statique (SRAM) dédiée au sein du Secure Enclave. Pour les opérations d'écriture, le moteur de protection de la mémoire *met à jour* le nonce et chaque niveau de l'arborescence d'intégrité jusqu'à la SRAM. Pour les opérations de lecture, le moteur de protection de la mémoire *vérifie* le nonce et chaque niveau de l'arborescence d'intégrité jusqu'à la SRAM. Les erreurs de correspondance du nonce sont traitées d'une façon similaire aux erreurs de correspondance de la balise d'authentification.

À partir des systèmes sur une puce A14 et M1 d'Apple, le moteur de protection de la mémoire prend en charge deux clés éphémères de protection de la mémoire. La première est utilisée pour les données confidentielles du Secure Enclave, et la deuxième est utilisée pour les données partagées avec le Neural Engine sécurisé.

Le moteur de protection de la mémoire fonctionne en phase et de façon transparente avec le Secure Enclave. Le Secure Enclave utilise la mémoire en lecture et en écriture comme s'il s'agissait d'une DRAM normale et non chiffrée, alors que tout observateur situé en dehors du Secure Enclave ne voit que la version chiffrée et authentifiée de la mémoire. En résulte une protection robuste de la mémoire sans contrepartie en matière de performance ou de complexité logicielle.

Mémoire morte d'amorçage du Secure Enclave

Le Secure Enclave comprend une mémoire morte d'amorçage dédiée. Semblable à la mémoire morte d'amorçage du processeur d'application, la mémoire morte d'amorçage du Secure Enclave est un code immuable qui établit la base matérielle sécurisée du Secure Enclave.

Lors du démarrage du système, iBoot assigne une zone de mémoire dédiée au Secure Enclave. Avant d'utiliser la mémoire, la mémoire morte d'amorçage du Secure Enclave initialise le moteur de protection de la mémoire pour fournir une protection cryptographique de la mémoire protégée du Secure Enclave.

Le processeur d'application envoie ensuite l'image de sepOS à la mémoire morte d'amorçage du Secure Enclave. Après avoir copié l'image de sepOS dans la mémoire protégée du Secure Enclave, la mémoire morte d'amorçage du Secure Enclave vérifie le hachage cryptographique et la signature de l'image pour vérifier que l'exécution de sepOS est autorisée sur l'appareil. Si l'image de sepOS est correctement signée pour être exécutée sur l'appareil, la mémoire morte d'amorçage du Secure Enclave transmet le contrôle à sepOS. Si la signature n'est pas valide, la mémoire morte d'amorçage du Secure Enclave est conçue pour empêcher toute utilisation du Secure Enclave jusqu'au prochain redémarrage de la puce.

Sur les systèmes sur une puce A10 et de génération ultérieure d'Apple, la mémoire morte d'amorçage du Secure Enclave verrouille un hachage de sepOS dans un registre dédié à cette fin. L'accélérateur de clé publique utilise ce hachage pour les clés liées au système d'exploitation.

Moniteur de démarrage du Secure Enclave

Sur les systèmes sur une puce A13 et de génération ultérieure d'Apple, le Secure Enclave comprend un moniteur de démarrage conçu pour assurer une intégrité plus robuste du hachage de l'instance de sepOS démarrée.

Lors du démarrage du système, la configuration de la protection de l'intégrité du coprocesseur système (SCIP) du Secure Enclave contribue à empêcher le processeur de ce dernier d'exécuter tout code qui ne provient pas de la mémoire morte d'amorçage du Secure Enclave. Le moniteur de démarrage contribue à empêcher le Secure Enclave de modifier directement la configuration de la SCIP. Pour que l'instance de sepOS chargée puisse s'exécuter, la mémoire morte d'amorçage du Secure Enclave envoie au moniteur de démarrage une requête accompagnée de l'adresse et de la taille de l'instance de sepOS chargée. À la réception de la requête, le moniteur de démarrage réinitialise le processeur Secure Enclave, hache l'instance de sepOS chargée, actualise les réglages de la SCIP pour permettre l'exécution de l'instance de sepOS chargée, puis lance l'exécution dans le code qui vient d'être chargé. Pendant que le système poursuit son démarrage, le même processus est employé chaque fois qu'un nouveau code est rendu exécutable. Chaque fois, le moniteur de démarrage met à jour un hachage d'exécution du processus de démarrage. Le moniteur de démarrage inclut aussi des paramètres de sécurité essentiels dans le hachage d'exécution.

Lorsque le démarrage est terminé, le moniteur de démarrage termine le hachage d'exécution et l'envoie à l'accélérateur de clé publique pour être utilisé avec les clés liées au système d'exploitation. Ce processus est conçu de sorte que la liaison des clés du système d'exploitation ne puisse pas être contournée, même en cas de vulnérabilité de la mémoire morte d'amorçage du Secure Enclave.

Générateur de nombres aléatoires matériel

Le TRNG (True Random Number Generator, générateur de nombres aléatoires matériel) est utilisé pour générer des données aléatoires sécurisées. Le Secure Enclave utilise le TRNG chaque fois qu'il génère une clé cryptographique aléatoire, une graine de clé aléatoire ou une autre entropie. Le TRNG repose sur plusieurs générateurs de créneaux post-traités avec l'algorithme CTR_DRBG (qui repose sur des chiffrements par blocs en mode compteur).

Clés cryptographiques racines

Le Secure Enclave comprend une clé cryptographique racine d'UID (Unique ID, identifiant unique). L'UID est unique à chaque appareil et n'est associé à aucun autre identifiant sur l'appareil.

Un UID aléatoire est fusionné au système sur une puce pendant la fabrication. À partir des systèmes sur une puce A9, l'UID est généré par le TRNG du Secure Enclave pendant la fabrication et inscrit dans les « fusibles » au moyen d'un processus logiciel qui s'exécute entièrement dans le Secure Enclave. Ce processus empêche l'UID d'être visible en dehors de l'appareil au cours de sa fabrication, de sorte que ni Apple ni ses fournisseurs ne peuvent y accéder ou le stocker.

sepOS utilise l'UID pour protéger les secrets propres à l'appareil. L'UID permet d'associer des données à un appareil précis de manière cryptographique. Par exemple, la hiérarchie des clés protégeant le système de fichiers comprend l'UID. De la sorte, si le stockage SSD interne est physiquement déplacé d'un appareil à un autre, les fichiers sont inaccessibles. Les autres secrets protégés propres à l'appareil comprennent les données de Touch ID ou de Face ID. Sur un Mac, seul le stockage entièrement interne associé au moteur AES bénéficie de ce niveau de chiffrement. Par exemple, ni les dispositifs de stockage externes connectés par USB ni le stockage PCIe ajouté au Mac Pro 2019 ne sont chiffrés de cette façon.

Le Secure Enclave comporte également un GID (Group ID, identifiant de groupe) d'appareil, qui est commun à tous les appareils dotés d'un système sur une puce donné. Par exemple, tous les appareils équipés du système sur une puce A14 d'Apple partagent le même GID.

L'UID et le GID ne sont pas accessibles par JTAG (Joint Test Action Group) ni d'autres interfaces de débogage.

Moteur AES du Secure Enclave

Le moteur AES du Secure Enclave est un bloc matériel qui sert à la cryptographie symétrique basée sur l'algorithme AES. Il est conçu pour résister aux fuites d'information résultant d'une attaque temporelle ou d'une attaque par analyse de consommation simple. À partir du système sur une puce A9, le moteur AES prévoit aussi des contre-mesures pour parer les attaques par analyse de consommation différentielle.

Le moteur AES prend en charge les clés matérielles et logicielles. Les clés matérielles sont dérivées de l'UID ou du GID du Secure Enclave. Ces clés ne quittent pas le moteur AES et ne sont pas rendues visibles, ni même par le logiciel sepOS. Bien que le logiciel puisse requérir des opérations de chiffrement et de déchiffrement au moyen des clés matérielles, il ne peut pas extraire les clés.

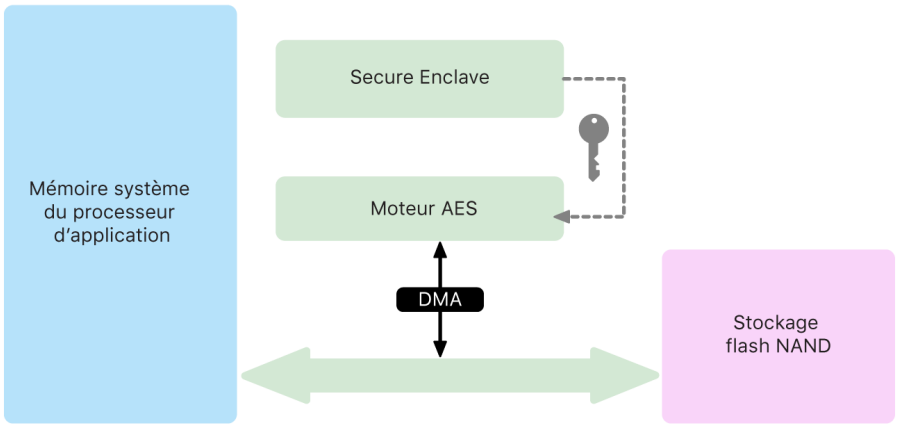
Sur les systèmes sur une puce A10 et de génération ultérieure d'Apple, le moteur AES comprend des bits de départ verrouillables qui diversifient les clés dérivées de l'UID ou du GID. Cela permet de conditionner l'accès aux données selon le mode de fonctionnement de l'appareil. Par exemple, des bits de départ verrouillables sont utilisés pour refuser l'accès aux données protégées par un mot de passe lors du démarrage en mode DFU (Device Firmware Upgrade, mise à niveau du programme interne de l'appareil). Pour en savoir plus, consultez la section Codes et mots de passe.

Moteur AES

Chaque appareil Apple équipé d'un Secure Enclave est doté d'un moteur de chiffrement AES256 dédié (le « moteur AES ») intégré dans le chemin DMA (Direct Memory Access, accès direct à la mémoire) entre le stockage flash NAND (non volatil) et la mémoire principale du système, ce qui rend le chiffrement des fichiers extrêmement efficace. Sur les processeurs A9 et de génération ultérieure de la série A, le sous-système de stockage flash se trouve sur un bus isolé qui est uniquement autorisé à accéder à la mémoire contenant les données utilisateur par le moteur de chiffrement DMA.

Lors du démarrage, sepOS génère une clé d'encapsulation éphémère avec le TRNG. Le Secure Enclave transmet cette clé au moteur AES via des fils dédiés, conçus pour empêcher tout logiciel à l'extérieur d'y accéder. sepOS peut ensuite utiliser la clé d'encapsulation éphémère pour envelopper les clés de fichier afin qu'elles soient utilisées par le pilote du système de fichiers du processeur d'application. Lorsque le pilote du système de fichiers lit ou écrit un fichier, il envoie la clé enveloppée au moteur AES, qui la débloque. Le moteur AES n'expose jamais la clé débloquée au logiciel.

Remarque : Le moteur AES est un composant indépendant du Secure Enclave et du moteur AES du Secure Enclave, mais son fonctionnement est étroitement lié au Secure Enclave, comme le montre le diagramme suivant.



Le moteur AES prend en charge le chiffrement pleine vitesse sur le chemin DMA pour assurer un chiffrement et un déchiffrement efficaces des données pendant l'écriture ou la lecture sur le stockage.

Accélérateur de clé publique

Le PKA (Public Key Accelerator, accélérateur de clé publique) est un bloc matériel utilisé pour effectuer des opérations de cryptographie asymétriques. Le PKA prend en charge les algorithmes de signature et de chiffrement RSA et ECC (Elliptic Curve Cryptography, cryptographie sur les courbes elliptiques). Le PKA est conçu pour résister aux fuites d'information résultant d'une attaque par canal auxiliaire (attaque temporelle, par analyse de consommation simple ou par analyse de consommation différentielle).

Le PKA prend en charge les clés logicielles et matérielles. Les clés matérielles sont dérivées de l'UID ou du GID du Secure Enclave. Ces clés ne quittent pas le PKA et ne sont pas rendues visibles, ni même par le logiciel sepOS.

À partir des systèmes sur une puce A13, les applications du chiffrement du PKA se sont avérées mathématiquement correctes selon les techniques de vérification formelle.

Sur les systèmes sur une puce A10 et de génération ultérieure d'Apple, le PKA prend en charge les clés liées au système d'exploitation, sous l'appellation protection scellée des clés (SKP). Ces clés sont générées à partir d'une combinaison de l'UID de l'appareil et du hachage de l'instance de sepOS en cours d'exécution sur l'appareil. Le hachage est fourni par la mémoire morte d'amorçage du Secure Enclave ou son moniteur de démarrage sur le système sur une puce A13 ou de génération ultérieure d'Apple. Ces clés servent à vérifier la version de sepOS au moment d'envoyer des requêtes à certains services Apple. Elles sont également utilisées pour améliorer la sécurité des données protégées par code en empêchant l'accès au matériel de chiffrement lorsque des modifications critiques sont apportées au système sans l'autorisation de l'utilisateur.

Stockage non volatil sécurisé

Le Secure Enclave est équipé d'un dispositif de stockage non volatil sécurisé dédié. Ce stockage est connecté au Secure Enclave au moyen d'un bus I2C dédié de sorte que seul le Secure Enclave peut y accéder. Toutes les clés de chiffrement des données de l'utilisateur sont associées à l'entropie qui y est stockée.

Sur les appareils équipés d'un système sur une puce A12, S4 ou de génération ultérieure, le Secure Enclave est couplé à un composant de stockage sécurisé réservé à l'entropie. Le composant de stockage sécurisé est lui-même doté d'un code immuable en mémoire morte, d'un générateur de nombres aléatoires matériel, d'une clé de chiffrement unique à l'appareil, de moteurs de chiffrement et d'un détecteur de sabotage matériel. Le Secure et le composant de stockage sécurisé communiquent au moyen d'un protocole chiffré et authentifié qui donne un accès exclusif à l'entropie.

Les appareils commercialisés pour la première fois à partir de l'automne 2020 sont équipés d'un composant de stockage sécurisé de deuxième génération. Ce nouveau composant de stockage sécurisé ajoute des référentiels sécurisés de compteur. Chaque référentiel sécurisé de compteur stocke un salage de 128 bits, un vérificateur de code de 128 bits, un compteur de 8 bits et une valeur maximale de tentative de 8 bits. Les référentiels sécurisés de compteur sont accessibles au moyen d'un protocole chiffré et authentifié.

Les référentiels sécurisés de compteur détiennent l'entropie requise pour déverrouiller les données utilisateur protégées par code. Pour accéder aux données utilisateur, le Secure Enclave jumelé doit dériver la valeur d'entropie du code à partir du code de l'utilisateur et de l'UID du Secure Enclave. Le code de l'utilisateur ne peut pas être appris au moyen des tentatives de déverrouillage provenant d'une source autre que le Secure Enclave jumelé. Si la limite de tentatives est atteinte (par exemple 10 sur iPhone), le composant de stockage sécurisé efface complètement les données protégées par code.

Pour créer un référentiel sécurisé de compteur, le Secure Enclave envoie au composant de stockage sécurisé la valeur d'entropie du code et le nombre maximal de tentatives. Le composant de stockage sécurisé génère la valeur de salage au moyen du générateur de nombres aléatoires. Il dérive ensuite une valeur de vérification du code et une valeur d'entropie du référentiel sécurisé à partir de l'entropie du code, de la clé de chiffrement unique du composant de stockage sécurisé et de la valeur de salage fournies. Le composant de stockage sécurisé initialise le référentiel sécurisé du compteur avec un compteur à zéro, le nombre maximal de tentatives, la valeur de vérification du code dérivée et la valeur de salage. Le composant de stockage sécurisé renvoie ensuite la valeur d'entropie générée du référentiel sécurisé au Secure Enclave.

Pour extraire la valeur d'entropie du référentiel sécurisé à partir d'un référentiel sécurisé de compteur, le Secure Enclave envoie l'entropie du code au composant de stockage sécurisé. Celui-ci incrémente d'abord le compteur du référentiel sécurisé. Si le compteur incrémenté dépasse la valeur maximale de tentatives, le composant de stockage sécurisé efface complètement le référentiel sécurisé de compteur. Si le nombre maximal de tentatives n'a pas été atteint, le composant de stockage sécurisé essaie de déduire la valeur de vérification du code et la valeur d'entropie du référentiel sécurisé avec le même algorithme que celui utilisé pour créer le référentiel sécurisé de compteur. Si la valeur de vérification du code déduite correspond à la valeur de vérification du code stockée, le composant de stockage sécurisé renvoie la valeur d'entropie au Secure Enclave et remet le compteur à zéro.

Les clés utilisées pour accéder aux données protégées par mot de passe sont enracinées dans l'entropie stockée dans les référentiels sécurisés de compteur. Pour en savoir plus, consultez la section Aperçu de la protection des données.

Le stockage non volatil sécurisé est utilisé pour tous les services antirejeu dans le Secure Enclave. Les services antirejeu du Secure Enclave servent à révoquer les données lorsque des événements dépassent les limites antirejeu, par exemple :

- Changement de code
- Activation ou désactivation de Touch ID ou de Face ID
- Ajout ou suppression d'une empreinte Touch ID ou d'un visage Face ID
- Réinitialisation de Touch ID ou de Face ID
- Ajout ou suppression d'une carte Apple Pay
- Suppression de tous les contenus et réglages

Sur les architectures qui ne disposent pas d'un composant de stockage sécurisé, c'est une mémoire EEPROM (mémoire morte programmable effaçable électriquement) qui fournit des services de stockage sécurisés pour le Secure Enclave. Tout comme les composants de stockage sécurisés, la mémoire EEPROM est attachée au Secure Enclave et est accessible uniquement à partir de celui-ci. Par contre, elle ne comporte pas de fonctionnalités de sécurité matérielle dédiée, elle ne garantit pas un accès exclusif à l'entropie (exception faite de ses caractéristiques de lien physique) et elle n'offre aucune fonctionnalité de référentiel sécurisé de compteur.

Neural Engine sécurisé

Sur les appareils équipés de Face ID, le Neural Engine sécurisé convertit les images 2D et les cartes de profondeur en une représentation mathématique du visage de l'utilisateur.

Sur les systèmes sur une puce A11 à A13, le Neural Engine sécurisé est intégré au Secure Enclave. Le Neural Engine sécurisé utilise l'accès direct à la mémoire (DMA) pour plus de performance. Une unité de gestion de la mémoire d'entrée/sortie (UGMES) sous le contrôle du noyau de sepOS limite cet accès direct aux zones autorisées de la mémoire.

À partir des systèmes sur une puce A14 et M1, le Neural Engine sécurisé est implémenté sous la forme d'un mode sécurisé dans le Neural Engine du processeur d'application. Un contrôleur de sécurité matériel dédié bascule entre les tâches du processeur d'application et celles du Secure Enclave en réinitialisant l'état du Neural Engine à chaque transition afin de protéger les données de Face ID. Un moteur dédié procède au chiffrement de la mémoire, à l'authentification et au contrôle d'accès. Simultanément, il utilise une clé de chiffrement et un intervalle de mémoire distincts pour restreindre les opérations du Neural Engine sécurisé aux zones de mémoire autorisées.

Contrôleur de puissance et contrôleur d'horloge

Tous les composants électroniques sont conçus pour fonctionner dans une enveloppe où la tension et la fréquence sont limitées. À l'extérieur de cette enveloppe, ils peuvent dysfonctionner et favoriser le contournement des contrôles de sécurité. Pour contribuer au maintien d'une tension et d'une fréquence sécuritaires, le Secure Enclave comporte des circuits de surveillance. Ceux-ci ont une enveloppe de fonctionnement beaucoup plus grande que le reste du Secure Enclave. Si les contrôleurs détectent un point de fonctionnement illégal, les horloges du Secure Enclave s'arrêtent automatiquement et ne redémarrent pas avant la prochaine réinitialisation du système sur une puce.

Résumé des fonctionnalités du Secure Enclave

Remarque : Les produits équipés du système sur une puce A12, A13, S4 ou S5 commercialisés pour la première fois à l'automne 2020 sont dotés du composant de stockage sécurisé de deuxième génération, tandis que les produits équipés de ces mêmes systèmes sur une puce commercialisés avant sont dotés d'un composant de stockage sécurisé de première génération.

Système sur une puce	Moteur de protection de la mémoire	Stockage sécurisé	Moteur AES	PKA
A8	Chiffrement et authentification	Mémoire EEPROM	Oui	Non
A9	Chiffrement et authentification	Mémoire EEPROM	Protection DPA	Oui
A10	Chiffrement et authentification	Mémoire EEPROM	Protection DPA et bits de départ verrouillables	Clés liées au système d'exploitation
A11	Chiffrement, authentification et prévention des rejeux	Mémoire EEPROM	Protection DPA et bits de départ verrouillables	Clés liées au système d'exploitation
A12 (appareils Apple commercialisés avant l'automne 2020)	Chiffrement, authentification et prévention des rejeux	Composant de stockage sécurisé (1re génération)	Protection DPA et bits de départ verrouillables	Clés liées au système d'exploitation
A12 (appareils Apple commercialisés après l'automne 2020)	Chiffrement, authentification et prévention des rejeux	Composant de stockage sécurisé (2e génération)	Protection DPA et bits de départ verrouillables	Clés liées au système d'exploitation

Système sur une puce	Moteur de protection de la mémoire	Stockage sécurisé	Moteur AES	PKA
A13 (appareils Apple commercialisés avant l'automne 2020)	Chiffrement, authentification et prévention des rejeux	Composant de stockage sécurisé (1re génération)	Protection DPA et bits de départ verrouillables	Clés liées au système d'exploitation et moniteur de démarrage
A13 (appareils Apple commercialisés après l'automne 2020)	Chiffrement, authentification et prévention des rejeux	Composant de stockage sécurisé (2e génération)	Protection DPA et bits de départ verrouillables	Clés liées au système d'exploitation et moniteur de démarrage
A14	Chiffrement, authentification et prévention des rejeux	Composant de stockage sécurisé (2e génération)	Protection DPA et bits de départ verrouillables	Clés liées au système d'exploitation et moniteur de démarrage
S3	Chiffrement et authentification	Mémoire EEPROM	Protection DPA et bits de départ verrouillables	Oui
S4	Chiffrement, authentification et prévention des rejeux	Composant de stockage sécurisé (1re génération)	Protection DPA et bits de départ verrouillables	Clés liées au système d'exploitation
S5 (appareils Apple commercialisés avant l'automne 2020)	Chiffrement, authentification et prévention des rejeux	Composant de stockage sécurisé (1re génération)	Protection DPA et bits de départ verrouillables	Clés liées au système d'exploitation
S5 (appareils Apple commercialisés après l'automne 2020)	Chiffrement, authentification et prévention des rejeux	Composant de stockage sécurisé (2e génération)	Protection DPA et bits de départ verrouillables	Clés liées au système d'exploitation
S6	Chiffrement, authentification et prévention des rejeux	Composant de stockage sécurisé (2e génération)	Protection DPA et bits de départ verrouillables	Clés liées au système d'exploitation
T2	Chiffrement et authentification	Mémoire EEPROM	Protection DPA et bits de départ verrouillables	Clés liées au système d'exploitation
M1	Chiffrement, authentification et prévention des rejeux	Composant de stockage sécurisé (2e génération)	Protection DPA et bits de départ verrouillables	Clés liées au système d'exploitation et moniteur de démarrage

Touch ID et Face ID

Sécurité de Touch ID et de Face ID

Les codes et les mots de passe sont essentiels pour la sécurité des appareils Apple. En même temps, les utilisateurs doivent être en mesure d'accéder rapidement à leurs appareils, parfois plus de 100 fois par jour. L'authentification biométrique permet de préserver la sécurité d'un code fort (ou même de renforcer le code ou le mot de passe, car il n'a pas à être entré manuellement), tout en offrant la commodité du déverrouillage rapide en un toucher ou regard. Touch ID et Face ID ne remplacent pas un code ou un mot de passe, mais ils accélèrent et facilitent l'accès dans la plupart des situations.

L'architecture d'identification biométrique d'Apple dépend d'une séparation stricte des responsabilités entre le capteur biométrique et le Secure Enclave, ainsi que d'une connexion sécurisée entre les deux. Le capteur capture l'image biométrique et la transmet en toute sécurité au Secure Enclave. Pendant l'inscription, le Secure Enclave traite, chiffre et stocke les données de modèle correspondantes de Touch ID et de Face ID. Pendant la mise en correspondance, le Secure Enclave compare les données entrantes du capteur biométrique aux modèles stockés afin de décider de déverrouiller l'appareil ou de répondre qu'une correspondance est valide (pour Apple Pay, dans les apps et pour d'autres utilisations de Touch ID et de Face ID). L'architecture prend en charge les appareils dotés du capteur et du Secure Enclave (comme l'iPhone, l'iPad et plusieurs systèmes Mac), et capables de séparer physiquement le capteur dans un périphérique qui est ensuite jumelé en toute sécurité au Secure Enclave sur un Mac avec puce Apple.

Touch ID

Touch ID est le système de lecture d'empreintes digitales qui permet de sécuriser rapidement et facilement l'accès aux appareils Apple compatibles. Cette technologie lit les empreintes digitales sous tous les angles et apprend à mieux les reconnaître au fil du temps, le capteur continuant à enrichir la carte de l'empreinte chaque fois qu'un nœud commun supplémentaire est détecté.

Les appareils Apple dotés d'un capteur Touch ID peuvent être déverrouillés à l'aide d'une empreinte digitale. Touch ID ne remplace pas le code de sécurité de l'appareil ni le mot de passe de l'utilisateur, toujours requis pour déverrouiller l'appareil après la mise en marche, le redémarrage ou encore la fermeture d'une session sur un Mac. Dans certaines apps, Touch ID peut être utilisé à la place du code ou du mode de passe de l'appareil, par exemple pour déverrouiller les notes protégées par mot de passe dans l'app Notes, pour déverrouiller les sites Web protégés par le trousseau et pour déverrouiller les apps prises en charge. Cependant, un code d'appareil ou un mot de passe utilisateur est systématiquement requis dans certains cas (comme pour modifier un code ou un mot de passe utilisateur, ou pour supprimer les inscriptions d'empreintes ou en créer de nouvelles).

Lorsque le lecteur d'empreintes digitales détecte le contact d'un doigt, le dispositif d'imagerie avancé numérise l'empreinte et transmet l'image au Secure Enclave. Le canal utilisé pour sécuriser cette connexion varie, selon que le capteur Touch ID est intégré à l'appareil avec le Secure Enclave ou situé dans un périphérique séparé.

Alors que la numérisation de l'empreinte est vectorisée à des fins d'analyse, l'image tramée est stockée temporairement dans la mémoire chiffrée du Secure Enclave, puis elle est effacée. L'analyse fait appel à une cartographie angulaire de la direction des crêtes sous-cutanées, un processus avec perte qui élimine les données de minuties digitales nécessaires à la reconstruction de l'empreinte digitale réelle de l'utilisateur. Pendant l'inscription, la carte de nœuds qui en résulte est stockée dans un format chiffré lisible uniquement par le Secure Enclave comme modèle pour comparer les correspondances ultérieures, mais sans information d'identification. Ces données sont confinées dans l'appareil. Elles ne sont pas envoyées à Apple ni incluses dans les sauvegardes de l'appareil.

Sécurité du canal du capteur Touch ID intégré

La communication entre le Secure Enclave et le capteur Touch ID intégré se fait par l'entremise d'un bus d'interface périphérique série. Le processeur transmet les données au Secure Enclave, mais ne peut pas les lire. Elles sont chiffrées et authentifiées avec une clé de session négociée à l'aide de la clé partagée attribuée à chaque capteur Touch ID et grâce au coprocesseur Secure Enclave correspondant en usine. Pour chaque capteur Touch ID, la clé partagée est robuste, aléatoire et différente. L'échange de la clé de session fait appel à l'algorithme d'enveloppement de clé AES, les deux parties fournissant une clé aléatoire qui établit la clé de session, et à un chiffrement des transmissions (avec AES-CCM) qui assure à la fois l'authentification et la confidentialité.

Sécurité de Face ID

Un regard suffit pour que Face ID déverrouille de façon sécurisée les appareils Apple compatibles. L'authentification intuitive et sécurisée est rendue possible par le système caméra TrueDepth, qui utilise des technologies avancées pour cartographier avec précision la géométrie du visage de l'utilisateur. Face ID exploite des réseaux neuronaux pour déterminer l'attention de l'utilisateur, établir la correspondance, prévenir la mystification et ainsi faire en sorte que l'utilisateur puisse déverrouiller son téléphone d'un seul regard. Face ID s'adapte automatiquement aux changements d'apparence de l'utilisateur et protège avec soin ses données biométriques.

La technologie Face ID a été conçue pour valider l'attention de l'utilisateur, offrir une solution fiable d'authentification dont le taux de correspondance erronée est faible et réduire les risques de mystification numérique ou physique.

Avec Face ID, la caméra TrueDepth cherche automatiquement le visage de l'utilisateur lorsque celui-ci réactive son appareil en l'élevant ou en touchant l'écran, et lorsque l'appareil tente d'authentifier l'utilisateur pour afficher une notification ou qu'une app prise en charge requiert l'authentification par Face ID. Lorsqu'un visage est détecté, Face ID valide l'attention et l'intention de déverrouiller l'appareil en vérifiant que les yeux de l'utilisateur sont ouverts et que son regard est dirigé vers l'appareil. Pour favoriser l'accessibilité, la vérification de l'attention par Face ID est désactivée lorsque VoiceOver est activé. Si nécessaire, cette fonctionnalité peut être désactivée séparément.

Une fois qu'elle a validé la présence d'un visage attentif, la caméra TrueDepth projette et analyse plus de 30 000 points infrarouges afin de créer une carte de profondeur du visage de l'utilisateur, accompagnée d'une image infrarouge 2D. Ces données sont utilisées pour créer une séquence d'images 2D et des cartes de profondeur, qui sont signées numériquement et envoyées au Secure Enclave. Pour contrer les tentatives de mystification numérique et physique, la caméra TrueDepth ordonne aléatoirement la séquence d'images 2D et les cartes de profondeur pour projeter un modèle aléatoire propre à l'appareil. Une partie du Neural Engine sécurisé, à l'abri dans le Secure Enclave, transforme ces données en une représentation mathématique et compare cette dernière aux données faciales enregistrées. Ces données faciales enregistrées forment elles-mêmes une représentation mathématique du visage de l'utilisateur obtenue à partir d'une série de poses.

Clavier Magic Keyboard doté de Touch ID

Le clavier Magic Keyboard doté de Touch ID (et le clavier Magic Keyboard doté de Touch ID et d'un pavé numérique) offre un capteur Touch ID sur un clavier externe compatible avec tout Mac doté d'une puce Apple. Le clavier Magic Keyboard doté de Touch ID joue le rôle d'un capteur biométrique. Il ne stocke aucun modèle biométrique, n'effectue pas la mise en correspondance et n'applique pas les règlements de sécurité (par exemple, l'obligation de saisir le mot de passe après 48 heures sans déverrouillage). Le capteur Touch ID du clavier Magic Keyboard doté de Touch ID doit être jumelé en toute sécurité au Secure Enclave sur le Mac avant que son utilisation soit possible. Le Secure Enclave procède ensuite aux opérations d'inscription et de mise en correspondance avant d'appliquer les règlements de sécurité de la même façon qu'il le ferait pour un capteur Touch ID intégré. Apple exécute le processus de jumelage à l'usine pour un clavier Magic Keyboard doté de Touch ID compris avec un Mac. L'utilisateur peut se charger du jumelage au besoin. Un clavier Magic Keyboard doté de Touch ID peut être jumelé en toute sécurité à un seul Mac à la fois, mais un Mac peut conserver les jumelages sécurisés d'un maximum de claviers Magic Keyboard dotés de Touch ID.

Le clavier Magic Keyboard doté de Touch ID est compatible avec les capteurs Touch ID intégrés. Si un doigt inscrit par le capteur Touch ID d'un Mac est présenté sur un clavier Magic Keyboard doté de Touch ID, le Secure Enclave sur un Mac peut traiter la correspondance et vice versa.

Afin de prendre en charge le jumelage sécurisé et, par le fait même, la communication entre le Secure Enclave du Mac et le clavier Magic Keyboard doté de Touch ID, ce dernier est doté d'un bloc matériel d'accélérateur de clé publique (PKA) pour fournir l'attestation, et de clés basées sur le matériel pour exécuter les processus cryptographiques nécessaires.

Jumelage sécurisé

Avant qu'un clavier Magic Keyboard doté de Touch ID puisse être utilisé pour les opérations de Touch ID, il doit être jumelé au Mac en toute sécurité. Pour le jumelage, le Secure Enclave sur le Mac et le bloc PKA du clavier Magic Keyboard doté de Touch ID échangent des clés publiques, associées à l'autorité de certification de confiance d'Apple, puis ils ont recours à des clés d'attestation matérielles et des clés ECDH éphémères pour attester leur identité en toute sécurité. Sur le Mac, ces données sont protégées par le Secure Enclave; sur le clavier Magic Keyboard doté de Touch ID, elles sont protégées par le bloc PKA. Après le jumelage sécurisé, toute communication entre le Mac et le clavier Magic Keyboard doté de Touch ID est chiffrée par l'algorithme AES-GCM, avec des clés ECDH éphémères basées sur les identités stockées.

Intention de jumelage sécurisée

Afin d'exécuter certaines opérations de Touch ID pour la première fois, comme l'inscription d'une nouvelle empreinte digitale, l'utilisateur doit confirmer physiquement son intention d'utiliser un clavier Magic Keyboard doté de Touch ID avec le Mac. L'intention est confirmée physiquement en appuyant deux fois sur le bouton d'alimentation du Mac lorsque l'interface utilisateur le demande, ou si une empreinte déjà inscrite sur le Mac est mise en correspondance. Pour en savoir plus, consultez la section Intention sécurisée et connexions au Secure Enclave.

Les transactions Apple Pay peuvent être autorisées au moyen d'une mise en correspondance Touch ID, ou en saisissant le mot de passe de l'utilisateur de macOS avant d'appuyer deux fois sur le bouton Touch ID du clavier Magic Keyboard doté de Touch ID. Cette dernière option permet à l'utilisateur de confirmer physiquement son intention même sans la mise en correspondance Touch ID.

Sécurité du canal du clavier Magic Keyboard doté de Touch ID

Pour contribuer à garantir un canal de communication sécurisé entre le capteur Touch ID du clavier Magic Keyboard doté de Touch ID et le Secure Enclave sur le Mac jumelé, les conditions suivantes sont nécessaires :

- jumelage sécurisé décrit ci-dessus entre le bloc PKA du clavier Magic Keyboard doté de Touch ID et le Secure Enclave;
- canal sécurisé entre le capteur du clavier Magic Keyboard doté de Touch ID et son bloc PKA.

Le canal sécurisé entre le capteur du clavier Magic Keyboard doté de Touch ID et son bloc PKA est établi à l'usine au moyen d'une clé unique partagée entre les deux. (Le canal sécurisé entre le Secure Enclave sur les ordinateurs Mac avec Touch ID et leur capteur intégré est établi de la même façon.)

Touch ID, Face ID, les codes et les mots de passe

Pour utiliser Touch ID ou Face ID, l'utilisateur doit configurer son appareil de sorte qu'un code ou un mot de passe soit nécessaire pour le déverrouiller. Lorsque Touch ID ou Face ID détecte une correspondance, l'appareil de l'utilisateur se déverrouille sans demander le code ou le mot de passe. Cela rend l'utilisation d'un code ou d'un mot de passe plus long et complexe beaucoup plus pratique, car il n'est pas nécessaire de le saisir aussi souvent. Les technologies Touch ID et Face ID ne remplacent pas le code ou le mot de passe, mais elles facilitent l'accès à l'appareil tout en respectant des limites et des contraintes temporelles soigneusement réfléchies. Cet élément est important, car un code ou un mot de passe complexe constitue la base de la protection des données utilisateur par chiffrement offerte par l'iPhone, l'iPad, le Mac et l'Apple Watch.

Situations qui requièrent le code ou le mot de passe de l'appareil

Les utilisateurs peuvent utiliser leur code ou mot de passe en tout temps à la place de Touch ID ou Face ID. À l'inverse, certaines situations ne permettent pas la biométrie. Les opérations suivantes, critiques pour la sécurité, nécessitent toujours la saisie d'un code ou mot de passe :

- la mise à jour du logiciel;
- l'effacement de l'appareil;
- l'affichage ou la modification des réglages du code;
- l'installation de profils de configuration;
- le déverrouillage de la sous-fenêtre « Sécurité et confidentialité » des Préférences Système sur Mac;
- le déverrouillage de la sous-fenêtre « Utilisateurs et groupes » des Préférences Système sur Mac (si FileVault est activé).

Un code ou un mot de passe est également requis dans les situations suivantes :

- L'appareil vient juste d'être allumé ou redémarré.
- L'utilisateur s'est déconnecté de son compte Mac (ou ne s'est pas encore connecté).
- L'utilisateur n'a pas déverrouillé son appareil depuis plus de 48 heures.
- L'utilisateur n'a pas déverrouillé son appareil à l'aide de son code ou mot de passe depuis 156 heures (6,5 jours) et de la biométrie depuis 4 heures.
- L'appareil a reçu une commande de verrouillage à distance.
- L'utilisateur a quitté l'écran Éteindre/Urgence SOS en appuyant simultanément sur un des boutons de volume et le bouton de mise en veille pendant 2 secondes avant d'appuyer sur Annuler.
- Il y a 5 tentatives de correspondance biométrique infructueuses (cependant, par convivialité, l'appareil peut offrir de saisir un code ou un mot de passe à la place de la biométrie après quelques tentatives infructueuses).

Lorsque Touch ID ou Face ID est activé sur un iPhone ou un iPad, l'appareil se verrouille chaque fois qu'il se met en veille ou dès que le bouton de mise en veille est enfoncé. Pour réactiver l'appareil, Touch ID et Face ID doivent trouver une correspondance pour valider l'identité de l'utilisateur, ou le code doit être entré.

La probabilité qu'une personne choisie au hasard dans la population puisse déverrouiller l'iPhone, l'iPad ou le Mac d'un utilisateur est de 1 chance sur 50 000 avec Touch ID ou 1 sur 1 000 000 avec Face ID. Cette probabilité augmente lorsque plusieurs empreintes digitales ou visages sont ajoutés (jusqu'à 1 sur 10 000 pour 5 empreintes et jusqu'à 1 sur 500 000 pour 2 visages). Afin d'offrir un niveau de protection supplémentaire, Touch ID et Face ID autorisent uniquement 5 tentatives infructueuses de mise en correspondance avant d'exiger le code ou le mot de passe pour déverrouiller l'appareil ou le compte de l'utilisateur. Avec Face ID, la probabilité d'une correspondance erronée est différente pour les jumeaux, les frères et sœurs qui se ressemblent ainsi que les enfants de moins de 13 ans, chez qui les traits du visage peuvent ne pas être encore totalement développés. Si le risque de correspondance erronée inquiète l'utilisateur, Apple recommande l'utilisation d'un code pour l'authentification.

Sécurité de la correspondance faciale

La mise en correspondance faciale est effectuée dans le Secure Enclave à l'aide de réseaux neuronaux entraînés expressément à cette fin. Apple a mis au point les réseaux neuronaux de correspondance faciale à l'aide de plus d'un milliard d'images, y compris des images infrarouges (IR) et tridimensionnelles recueillies lors d'études réalisées avec le consentement éclairé des participants. Elle a ensuite travaillé avec des participants de par le monde pour inclure un groupe représentatif de personnes en tenant compte du sexe, de l'âge, de l'ethnicité et d'autres facteurs. Les études ont été approfondies selon les besoins afin de fournir un degré de précision élevé pour un large éventail d'utilisateurs. Face ID a été conçu pour détecter les chapeaux, les foulards, les lunettes, les verres de contact et de nombreux types de lunettes de soleil. En outre, cette technologie a été pensée pour fonctionner à l'intérieur, à l'extérieur et même dans l'obscurité totale. Un réseau neuronal supplémentaire entraîné pour déceler la mystification et y résister protège l'appareil contre les tentatives de déverrouillage à l'aide de photos ou de masques. Les données de Face ID, y compris les représentations mathématiques du visage de l'utilisateur, sont chiffrées et accessibles uniquement par le Secure Enclave. Ces données sont confinées dans l'appareil. Elles ne sont pas envoyées à Apple ni incluses dans les sauvegardes de l'appareil. Dans des situations normales d'utilisation, les données de Face ID suivantes sont enregistrées et chiffrées pour être utilisées uniquement par le Secure Enclave :

- les représentations mathématiques du visage de l'utilisateur calculées lors de la phase d'inscription;
- les représentations mathématiques du visage de l'utilisateur calculées lors de certaines tentatives de déverrouillage si Face ID les juge utiles pour améliorer la mise en correspondance.

Les images faciales obtenues lors des situations normales d'utilisation ne sont pas enregistrées. Elles sont effacées immédiatement après le calcul de la représentation mathématique utilisée lors de la phase d'inscription ou lors de comparaisons avec les données enregistrées dans Face ID.

Amélioration des correspondances de Face ID

Pour améliorer la performance de la correspondance et suivre les changements naturels du visage ou de l'apparence, Face ID élargit la représentation mathématique stockée au fil du temps. Après une correspondance réussie, Face ID peut utiliser la représentation mathématique nouvellement calculée, si sa qualité est jugée suffisante, pour un nombre déterminé de correspondances supplémentaires avant d'effacer ces données. Inversement, si Face ID ne reconnaît pas un visage, mais que la qualité de la correspondance dépasse un certain seuil et que l'utilisateur réagit à l'échec en entrant son code, Face ID enregistre une nouvelle image et élargit ses données enregistrées en y ajoutant la représentation mathématique nouvellement calculée. Ces nouvelles données de Face ID sont effacées si l'utilisateur cesse d'y correspondre ou après un nombre déterminé de correspondances. Ces processus d'élargissement permettent à Face ID de suivre les changements radicaux de la pilosité faciale ou du maquillage de l'utilisateur tout en réduisant les correspondances erronées.

Utilisations de Touch ID et de Face ID

Déverrouillage d'un appareil ou d'un compte utilisateur

Quand un appareil ou un compte se verrouille alors que Touch ID ou Face ID est désactivé, les clés de la classe la plus élevée de protection des données, qui sont stockées dans le Secure Enclave, sont effacées. Les fichiers et les éléments du trousseau appartenant à cette classe restent inaccessibles jusqu'à ce que l'utilisateur déverrouille l'appareil ou le compte en entrant son code ou son mot de passe.

Si Touch ID ou Face ID est activé, les clés ne sont pas effacées lorsque l'appareil ou le compte se verrouille; elles sont plutôt enveloppées avec une clé attribuée au sous-système de Touch ID ou de Face ID à l'intérieur du Secure Enclave. Lorsqu'un utilisateur tente de déverrouiller l'appareil ou le compte, si l'appareil détecte une correspondance, il fournit la clé permettant de développer les clés de protection des données. Ce processus apporte une protection supplémentaire, puisqu'il oblige les sous-systèmes de protection des données et Touch ID ou Face ID à coopérer pour déverrouiller l'appareil.

Lorsque l'appareil redémarre, les clés requises par Touch ID ou Face ID pour son déverrouillage ou celui du compte sont perdues; elles sont supprimées par le Secure Enclave dès qu'une condition nécessitant la saisie du code ou du mot de passe est remplie.

Sécurisation des achats effectués avec Apple Pay

L'utilisateur peut également utiliser Touch ID et Face ID avec Apple Pay pour effectuer des achats en toute simplicité et de façon sécuritaire dans des magasins, des apps et sur le Web :

- *Utilisation de Touch ID :* Avec Touch ID, l'intention de payer est confirmée par le geste qui active le capteur de Touch ID combiné à la mise en correspondance de l'empreinte de l'utilisateur.

- *Utilisation de Face ID en magasin :* Pour autoriser un paiement en magasin avec Face ID, l'utilisateur doit d'abord confirmer son intention de payer en appuyant deux fois sur le bouton latéral. Ce double-clic atteste l'intention de l'utilisateur au moyen d'un geste directement lié au Secure Enclave qui ne peut être imité par un processus malveillant. L'utilisateur s'authentifie ensuite avec Face ID avant de placer l'appareil à proximité du lecteur de paiement sans contact. Un mode de paiement Apple Pay différent peut être sélectionné après l'authentification par Face ID, ce qui nécessite une nouvelle authentification, mais l'utilisateur n'a pas à réappuyer deux fois sur le bouton latéral.
- *Utilisation de Face ID dans les apps et sur le Web :* Pour effectuer un paiement dans des apps ou sur le Web, l'utilisateur confirme son intention de payer en appuyant deux fois sur le bouton latéral, puis en s'authentifiant avec Face ID pour autoriser le paiement. Si la transaction Apple Pay n'est pas terminée 60 secondes après que l'utilisateur a appuyé deux fois sur le bouton latéral, l'utilisateur devra confirmer de nouveau son intention de payer en réappuyant deux fois sur le bouton.

Utilisation des API fournies par le système

Les apps tierces peuvent utiliser les API fournies par le système pour demander à l'utilisateur de s'authentifier à l'aide de Touch ID, de Face ID, d'un code ou d'un mot de passe. Les apps qui prennent en charge Touch ID prennent automatiquement en charge Face ID sans modification. Si la technologie Touch ID ou Face ID est utilisée, l'app n'est informée que de la réussite ou de l'échec de l'authentification, et elle ne peut pas accéder à Touch ID, à Face ID ou aux données associées à l'utilisateur.

Protection des éléments du trousseau

Les éléments du trousseau peuvent également être protégés par Touch ID ou Face ID; dans ce cas, le Secure Enclave ne permet d'y accéder que si une correspondance est validée, ou que le code de l'appareil ou le mot de passe du compte est saisi. Les développeurs d'apps ont aussi à leur disposition des API qui permettent de vérifier que l'utilisateur a choisi un code ou un mot de passe et qu'il peut donc s'authentifier ou déverrouiller les éléments du trousseau à l'aide de Touch ID ou de Face ID. Les développeurs d'apps peuvent :

- exiger que les opérations des API d'authentification ne passent pas par la saisie du mot de passe d'une application ou du code de l'appareil. Ils peuvent interroger le système pour savoir si un utilisateur est enregistré, ce qui permet d'utiliser Touch ID ou Face ID comme deuxième facteur dans les apps qui requièrent une sécurité accrue;
- générer et utiliser des clés basées sur la cryptographie sur les courbes elliptiques (ECC, Elliptic Curve Cryptography) dans le Secure Enclave qui peuvent être protégées par Touch ID ou Face ID. Les opérations avec ces clés se font toujours dans le Secure Enclave après que ce dernier a autorisé leur utilisation.

Achats et approbations connexes

Les utilisateurs peuvent également configurer Touch ID ou Face ID pour autoriser des achats dans l'iTunes Store, l'App Store, Apple Books et ailleurs, et ainsi éviter de saisir le mot de passe de leur identifiant Apple. Lorsque des achats sont effectués, le Secure Enclave vérifie qu'une autorisation biométrique a eu lieu, puis il présente les clés ECC utilisées pour signer la demande du magasin.

Intention sécurisée et connexions au Secure Enclave

L'intention sécurisée représente une façon de confirmer l'intention d'un utilisateur sans aucune interaction avec le système d'exploitation ou le processeur d'application. La connexion est un lien physique (entre un bouton et le Secure Enclave) présent sur les appareils suivants :

- iPhone X et modèles plus récents;
- Apple Watch Series 1 et modèles plus récents;
- iPad Pro (tous les modèles);
- iPad Air (2020);
- ordinateurs Mac avec puce Apple.

Grâce à ce lien, les utilisateurs peuvent confirmer leur intention d'effectuer une opération d'une façon conçue pour que même les logiciels avec privilèges racines ou exécutés dans le noyau ne peuvent pas mystifier.

Cette fonction sert à confirmer l'intention de l'utilisateur lors de transactions Apple Pay et pour finaliser le jumelage d'un clavier Magic Keyboard doté de Touch ID à un Mac avec puce Apple. Le fait d'appuyer deux fois sur le bouton approprié lorsque l'interface utilisateur le demande signale la confirmation de l'intention de l'utilisateur. Pour en savoir plus, consultez la section Sécurisation des achats effectués avec Apple Pay. Un mécanisme semblable, basé sur le Secure Enclave et le programme interne T2, est pris en charge par les modèles de MacBook sans Touch Bar dotés de la puce T2 Security d'Apple.

Déconnexion matérielle du micro

Tous les ordinateurs portables Mac dotés d'une puce Apple ou dotés d'un processeur Intel et d'une puce T2 Security d'Apple sont équipés d'un mécanisme de déconnexion matérielle qui désactive le micro lorsque l'écran est rabattu. Sur tous les ordinateurs portables MacBook Pro et MacBook Air de 13 pouces équipés de la puce T2, tous les ordinateurs portables MacBook équipés d'une puce T2 commercialisés à partir de 2019 et tous les ordinateurs portables Mac avec puce Apple, ce mécanisme de déconnexion est uniquement matériel. Il vise à empêcher tous les logiciels, même ceux avec des privilèges racines ou des privilèges du noyau sous macOS, et même le logiciel sur la puce T2 ou d'autres programmes internes, d'activer le microphone si l'écran est rabattu. (La caméra n'est pas déconnectée matériellement, car son champ de vision est complètement obstrué lorsque l'écran est rabattu.)

Les modèles d'iPad commercialisés à partir de 2020 sont aussi dotés de la fonction de déconnexion matérielle du micro. Lorsqu'un étui homologué MFi (y compris ceux vendus par Apple) installé sur un iPad est fermé, le micro est physiquement déconnecté, ce qui vise à empêcher la transmission des données audio du microphone à tout logiciel, même si celui-ci est doté des privilèges racines ou des privilèges du noyau sous iPadOS ou dans tout programme interne de l'appareil.

Les protections mentionnées dans cette section sont implémentées directement au moyen de réseaux logiques conformément au diagramme de circuit suivant.

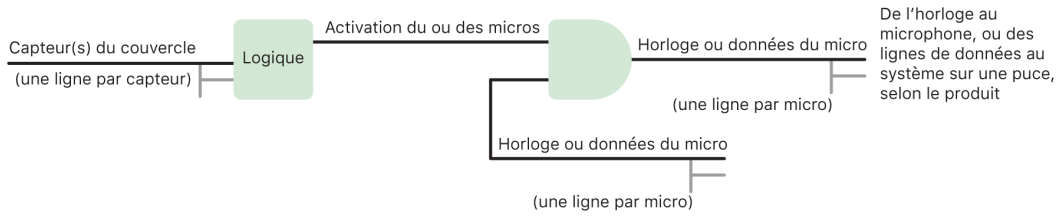


Diagramme du circuit.

Dans chaque produit doté d'un mécanisme matériel d'interruption du micro, un ou plusieurs capteurs détectent le rabattement de l'écran ou de l'étui au moyen d'une propriété physique (par exemple un capteur à effet Hall ou un capteur d'angle d'articulation) de l'interaction. Pour les capteurs qui requièrent un étalonnage, les paramètres sont configurés lors de la fabrication de l'appareil, et le processus d'étalonnage comprend un verrou matériel irréversible susceptible de s'enclencher après toute modification postérieure des paramètres sensibles du capteur. Ces capteurs émettent un signal matériel direct transmis par une simple logique matérielle non reprogrammable. Cette logique comprend des mécanismes d'antirebond, d'hystérésis ou de report de jusqu'à 500 ms avant de désactiver le micro. Selon le produit, ce signal peut être implémenté soit en désactivant les lignes qui transportent les données entre le micro et le système sur une puce, soit en désactivant une des lignes d'entrée du module du micro qui permettent à celui-ci d'être actif, par exemple celle de l'horloge ou un contrôle effectif semblable.

Mode Express pour les cartes accessibles en mode Réserve

Si iOS n'est pas en marche parce qu'iPhone est déchargé, la batterie a peut-être encore assez d'énergie pour permettre les transactions en mode Express. Sur les modèles d'iPhone qui le prennent en charge, ce mode fonctionne automatiquement avec :

- une carte de paiement ou de transport désignée comme carte de transport express;
- une carte étudiante pour laquelle le mode Express est activé;
- un laissez-passer de parc pour lequel le mode Express est activé;
- une clé de véhicule pour laquelle le mode Express est activé.

Il suffit d'appuyer sur le bouton latéral (ou, dans le cas de l'iPhone SE 2e génération, sur le bouton principal) pour que s'affichent l'icône de batterie faible et un message indiquant que des cartes sont utilisables en mode Express. Le contrôleur CCP exécute les transactions Express selon les mêmes conditions que lorsqu'iOS est en marche, sauf que les transactions sont signalées uniquement par une pulsation (aucune notification ne s'affiche). Sur l'iPhone SE 2e génération, les transactions effectuées peuvent mettre quelques secondes à s'afficher à l'écran. Cette fonctionnalité n'est pas disponible lorsque l'appareil a été éteint normalement par l'utilisateur.

Sécurité du système

Aperçu de la sécurité du système

Bien ancrées dans les composants matériels d'Apple, les fonctionnalités de sécurité contrôlent l'accès aux ressources système des appareils sans pour autant nuire à leur utilisation. La sécurité du système englobe le processus de démarrage, les mises à jour logicielles et la protection des ressources système comme le processeur central, la mémoire, le disque, les programmes et les données stockées.

Les plus récentes versions des systèmes d'exploitation Apple sont les plus sûres. Les fonctionnalités de sécurité reposent notamment sur le *démarrage sécurisé*, qui prévient les attaques de logiciels malveillants lorsque le système démarre. Le démarrage sécurisé, qui commence au niveau matériel, déclenche une chaîne de confiance au niveau logiciel – une chaîne dont chaque maillon est conçu pour vérifier que le suivant fonctionne correctement avant de lui céder le contrôle. Ce modèle de sécurité sous-tend, non seulement le démarrage par défaut des appareils Apple, mais aussi leurs divers modes de récupération et de mise à jour. Les sous-composants comme la puce T2 et le coprocesseur Secure Enclave procèdent également à leur propre démarrage sécurisé, de sorte que seul le code connu d'Apple s'exécute. Le système de mise à jour peut même contribuer à prévenir les tentatives de retour à une version antérieure du système d'exploitation, qui visent à dérober les données de l'utilisateur.

Enfin, les appareils Apple comportent des protections de démarrage et d'exécution qui assurent leur intégrité tout au long de leur utilisation. Les puces conçues par Apple sur iPhone, iPad, Apple Watch, Apple TV et HomePod, ainsi que celle intégrée à Mac, fournissent une architecture commune qui empêche la corruption des systèmes d'exploitation. macOS comprend également un éventail de protections configurables qui sous-tendent son modèle unique, ainsi que des fonctionnalités prises en charge par tous les Mac.

Démarrage sécurisé

Processus de démarrage pour les appareils iOS et iPadOS

À chaque étape du processus de démarrage, des composants à signature cryptographique Apple permettent une vérification de l'intégrité, de sorte que le démarrage a lieu uniquement une fois que la chaîne de confiance est établie. Ces composants comprennent les chargeurs d'amorçage, le noyau, les extensions du noyau et le programme interne de bande de base cellulaire. Cette chaîne de démarrage sécurisé est conçue pour vérifier que les niveaux les plus bas des logiciels ne sont pas altérés.

Au démarrage d'un appareil iOS ou iPadOS, le processeur d'application de ce dernier exécute immédiatement un programme stocké dans une mémoire en lecture seule appelée « mémoire morte d'amorçage ». Ce code immuable, qui fait office de *base matérielle sécurisée*, est défini pendant la fabrication de la puce et est implicitement digne de confiance. La mémoire morte d'amorçage contient la clé publique d'autorité de certification Apple Root, qui sert à vérifier que le chargeur d'amorçage iBoot est signé par Apple avant d'autoriser son chargement. Cette étape est la première d'une chaîne de confiance où chaque étape vérifie que le certificat de la suivante est bien signé par Apple. Lorsqu'iBoot termine ses tâches, il vérifie et exécute le noyau iOS ou iPadOS. Pour les appareils dotés d'un processeur A9 ou de génération antérieure de la série A, la mémoire morte d'amorçage charge et vérifie une étape de chargeur d'amorçage de niveau inférieur (LLB) supplémentaire qui à son tour charge et vérifie iBoot.

L'échec du chargement ou de la vérification des étapes suivantes est géré différemment selon le matériel :

- *La mémoire morte d'amorçage n'arrive pas à charger le LLB (sur les vieux appareils) :* mode de mise à niveau du programme interne de l'appareil (DFU);
- *LLB ou iBoot :* mode de récupération

Dans les deux cas, l'appareil doit être connecté au Finder (sous macOS 10.15 et les versions ultérieures) ou à iTunes (sous macOS 10.14 et les versions antérieures) par USB, et ses réglages d'origine par défaut, restaurés.

Le registre de progression du démarrage (BPR) est utilisé par le Secure Enclave pour limiter l'accès aux données des utilisateurs dans différents modes et est mis à jour avant le démarrage des modes suivants :

- *Mode DFU :* réglé par la mémoire morte d'amorçage sur les appareils dotés d'un système sur une puce A12 ou de génération ultérieure d'Apple.
- *Mode de récupération :* réglé par iBoot sur les appareils dotés d'un système sur une puce A10, S2 ou de génération ultérieure d'Apple.

Sur les appareils avec connectivité cellulaire, un sous-système de bande de base cellulaire effectue un démarrage sécurisé supplémentaire au moyen d'un logiciel et de clés signés et vérifiés par le processeur de bande de base.

Le Secure Enclave effectue également un démarrage sécurisé qui vérifie que son logiciel (sepOS) est vérifié et signé par Apple.

Implémentation iBoot à mémoire sécurisée

Sous iOS 14 et iPadOS 14, Apple a modifié la chaîne d'outils du compilateur C servant à élaborer le chargeur d'amorçage iBoot afin d'en améliorer la sécurité. La chaîne d'outils modifiée implémente du code est conçue pour prévenir les problèmes liés à la sûreté de la mémoire et du typage (ces problèmes sont courants parmi les programmes C). Par exemple, elle empêche la plupart des vulnérabilités des classes suivantes :

- les dépassements de la mémoire tampon, en veillant à ce que les pointeurs comportent des informations sur les limites qui seront vérifiées lors de l'accès à la mémoire;
- l'exploitation du tas, en séparant les données du tas de leurs métadonnées et en détectant précisément les conditions de l'erreur, telles qu'une double utilisation de la fonction free;

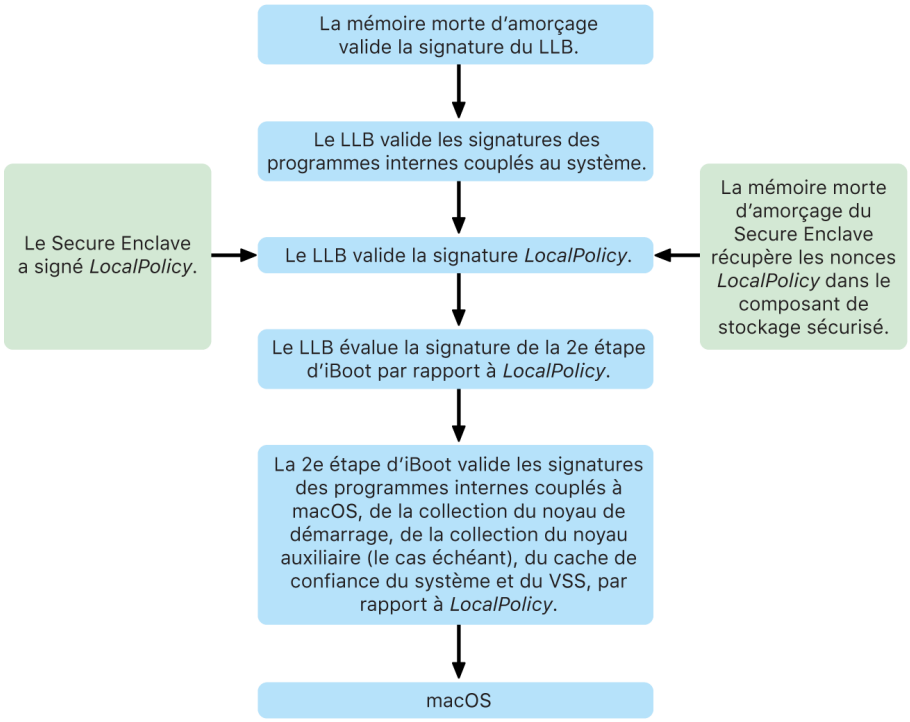
- la confusion de type, en veillant à ce que tous les pointeurs comportent des informations sur le type d'exécution qui seront vérifiées lors des opérations de conversion de type de pointeur;
- la confusion de type causée par des erreurs d'utilisation consécutive à une libération de la mémoire, en séparant toutes les attributions dynamiques de mémoire par type statique.

Cette technologie est disponible sur les iPhone équipés de la puce A13 Bionic d'Apple et les modèles plus récents, et sur les iPad équipés de la puce A14 Bionic.

Ordinateurs Mac avec puce Apple

Processus de démarrage d'un Mac avec puce Apple

Le démarrage d'un Mac avec puce Apple suit un processus semblable à celui d'un iPhone ou d'un iPad.



Étapes du processus de démarrage d'un Mac avec puce Apple.

Lors de la première étape de la chaîne de confiance, la puce exécute du code à partir de la mémoire morte d'amorçage. Le démarrage sécurisé de macOS sur un Mac avec puce Apple vérifie le code du système d'exploitation même ainsi que les règlements de sécurité et les extensions de noyau (ces dernières sont prises en charge, mais leur utilisation n'est pas recommandée) configurées par les utilisateurs autorisés.

Lorsque le LLB est lancé, il vérifie les signatures et charge les programmes internes couplés au système qui se rapportent aux cœurs du système sur une puce, comme les contrôleurs de stockage, d'affichage, de gestion système et Thunderbolt. Le LLB est également responsable du chargement du fichier LocalPolicy, qui est signé par le processeur Secure Enclave. Le fichier LocalPolicy décrit la configuration choisie par l'utilisateur pour démarrer le système ainsi que les règlements de sécurité de l'exécution. Le fichier LocalPolicy adopte le même format de structure de données que les autres objets de démarrage, sauf qu'au lieu d'être signé par un serveur central d'Apple (comme les mises à jour logicielles), il est signé localement par une clé privée qui est uniquement disponible au sein du Secure Enclave d'un ordinateur donné.

Pour contribuer à prévenir le rejeu de tout fichier LocalPolicy antérieur, le LLB doit chercher un nonce dans le composant de stockage sécurisé rattaché au Secure Enclave. Pour ce faire, il utilise la mémoire morte d'amorçage du Secure Enclave et vérifie que le nonce du fichier LocalPolicy correspond à celui du composant de stockage sécurisé. Cela contribue à empêcher tout ancien fichier LocalPolicy, dont le niveau de sécurité pourrait être inférieur, d'être de nouveau appliqué au système après que la sécurité a été mise à niveau. Par conséquent, le démarrage sécurisé d'un Mac avec puce Apple protège l'appareil de la rétrogradation du système d'exploitation et du règlement de sécurité tout à la fois.

Le fichier LocalPolicy détermine si la configuration de sécurité du système d'exploitation est maximale, réduite ou permissive.

- *Sécurité maximale :* Le système se comporte comme iOS et iPadOS, et permet uniquement le démarrage du logiciel déterminé comme étant le plus récent au moment de l'installation.
- *Sécurité réduite :* Le LLB est autorisé à approuver les signatures « globales » fournies avec le système d'exploitation. Cela permet au système d'exécuter des versions antérieures de macOS. On parle de sécurité *réduite*, car les versions antérieures de macOS comportent inévitablement des vulnérabilités non corrigées. Il s'agit du niveau de sécurité requis pour lancer des extensions de noyau.
- *Sécurité permissive :* Le système agit selon un niveau de sécurité semblable à la sécurité réduite, car il utilise une vérification des signatures globales pendant et après iBoot, mais il indique également à iBoot d'accepter que certains objets de démarrage soient signés par le Secure Enclave avec la clé qui sert aussi à signer le fichier LocalPolicy. Ce niveau de règlement sert aux utilisateurs qui conçoivent, signent et exécutent leurs propres noyaux XNU.

Si le fichier LocalPolicy indique au LLB que le système d'exploitation sélectionné s'exécute en mode Sécurité maximale, le LLB évalue la signature personnalisée d'iBoot. S'il s'exécute en mode Sécurité réduite ou en mode Sécurité permissive, le LLB évalue la signature globale. Toute erreur de validation de la signature forcera le démarrage de recoveryOS pour proposer des options de réparation à l'utilisateur.

Lorsque le LLB passe le relais à iBoot, ce dernier charge les programmes internes couplés à macOS, comme ceux notamment associés au Neural Engine sécurisé, au processeur toujours actif et à d'autres programmes internes. iBoot analyse également les informations relatives au fichier LocalPolicy transmis par le LLB. Si le fichier LocalPolicy indique qu'il doit y avoir une collection du noyau auxiliaire (AuxKC), iBoot la recherche dans le système de fichiers, vérifie qu'elle est signée par le Secure Enclave au moyen de la même clé que pour le fichier LocalPolicy et valide son hachage en le comparant à celui stocké dans le fichier LocalPolicy. Si l'AuxKC est valide, iBoot la place dans la mémoire avec la collection du noyau de démarrage avant de verrouiller au moyen de la protection de l'intégrité du coprocesseur système (SCIP, System Coprocessor Integrity Protection) toute la zone de mémoire qui couvre ces deux collections. Si la politique indique qu'une AuxKC doit être présente alors qu'elle est introuvable, le démarrage de macOS se poursuit tout en ignorant la collection en question. iBoot est également chargé de vérifier le hachage racine du volume système signé (VSS) pour confirmer la vérification complète de l'intégrité du système de fichiers que le noyau va monter.

Modes de démarrage d'un Mac avec puce Apple

Un Mac avec puce Apple dispose des modes de démarrage décrits ci-dessous.

Mode	Combinaison de touches	Description
macOS	Lorsque l'appareil est éteint, appuyez sur le bouton d'alimentation et **relâchez-le**.	1. La mémoire morte d'amorçage passe le relais au LLB. 2. Le LLB charge les programmes internes couplés au système ainsi que le fichier LocalPolicy de la version de macOS sélectionnée. 3. Le LLB transmet au registre de progression du démarrage (BPR) une donnée qui indique qu'un démarrage normal de macOS est en cours avant de passer le relais à iBoot. 4. iBoot charge les programmes internes couplés à mac OS, le cache statique de confiance, l'arborescence de l'appareil et la collection du noyau de démarrage. 5. Si le fichier LocalPolicy le permet, iBook charge la collection auxiliaire du noyau (AuxKC) des extensions du noyau tierces. 6. Si le fichier LocalPolicy ne l'a pas désactivé, iBoot valide le hachage de la signature racine du volume système signé (VSS).
recoveryOS	Lorsque l'appareil est éteint, appuyez **de façon prolongée** sur le bouton d'alimentation.	1. La mémoire morte d'amorçage passe le relais au LLB. 2. Le LLB charge les programmes internes couplés au système ainsi que le fichier LocalPolicy de recovery OS. 3. Le LLB transmet une donnée au registre de progression du démarrage qui indique que le démarrage de recoveryOS est en cours avant de passer le relais à iBoot pour démarrer recoveryOS. 4. iBoot charge les programmes internes couplés à macOS, le cache de confiance, l'arborescence de l'appareil et la collection du noyau de démarrage. *Remarque :* Le fichier LocalPolicy de recoveryOS ne permet pas de rétrograder la sécurité.

Mode	Combinaison de touches	Description
Démarrage de secours de recoveryOS	Lorsque l’appareil est éteint, **appuyez deux fois sur le bouton d’alimentation puis maintenez-le enfoncé**.	Il s’agit du même processus que le démarrage de recoveryOS, excepté qu’il démarre vers une deuxième copie de recoveryOS conservée à des fins de résilience. Cependant, le LLB ne transmet aucune donnée au registre de progression du démarrage qui indique que recoveryOS est en cours de démarrage. Par conséquent, le démarrage de secours de recovery OS ne permet pas de modifier l’état de sécurité du système.
Mode sans échec	Démarrez recoveryOS comme indiqué ci-dessus, puis maintenez la touche **Maj** enfoncée tout en sélectionnant le volume de démarrage.	1. Le démarrage de recoveryOS s’effectue comme décrit ci-dessus. 2. Le fait de maintenir la touche Maj enfoncée tout en sélectionnant un volume force l’application Boot Picker à valider cette version de macOS pour le démarrage, comme d’habitude, mais elle configure également une variable `nvram` qui commande à iBoot de ne pas charger l’AuxKC au démarrage suivant. 3. Le système redémarre sur le volume choisi, mais i Boot ne charge pas l’AuxKC.

Contrôle du règlement de sécurité du disque de démarrage d’un Mac avec puce Apple

Aperçu

Contrairement aux règlements de sécurité sur un Mac avec processeur Intel, ceux d’un Mac avec puce Apple s’appliquent au niveau de chaque système d’exploitation installé. Cela signifie que plusieurs instances de macOS de versions différentes peuvent bénéficier chacune de leur propre règlement de sécurité sur un même Mac. C’est pour cette raison qu’un sélecteur de système d’exploitation a été ajouté à l’utilitaire Sécurité au démarrage.

La sélection du stockage de macOS pour modifier le règlement de sécurité.

Sur un Mac avec puce Apple, l'utilitaire Sécurité système indique l'état de sécurité globale de macOS configuré par l'utilisateur, comme le démarrage d'une extension de noyau ou la configuration de la protection de l'intégrité du système. Si la modification d'un réglage de sécurité réduit considérablement la sécurité du système ou rend ce dernier plus vulnérable, l'utilisateur doit démarrer recoveryOS en maintenant le bouton d'alimentation enfoncé (de sorte qu'aucun logiciel malveillant ne puisse déclencher le signal et que seule une personne physiquement présente puisse procéder) pour procéder à la modification. C'est pourquoi un Mac avec puce Apple ne requiert ni ne prend en charge un mot de passe du programme interne. Toutes les modifications importantes requièrent déjà l'autorisation de l'utilisateur. Pour en savoir plus sur la protection de l'intégrité du système, consultez la rubrique Protection de l'intégrité du système.

Les réglages « Sécurité maximale » et « Sécurité réduite » peuvent être configurés avec l'utilitaire Sécurité au démarrage à partir de recoveryOS. En revanche, le réglage « Sécurité permissive » est accessible uniquement à partir des outils de ligne de commande pour les utilisateurs qui acceptent le risque de réduire considérablement la sécurité de leur Mac.

Règlement Sécurité maximale

« Sécurité maximale » est le réglage par défaut et se comporte comme iOS et iPadOS. Lors du téléchargement du logiciel et de la préparation de son installation, plutôt que d'utiliser la signature globale qui l'accompagne, macOS communique avec le même serveur de signature Apple utilisé par iOS et iPadOS, et demande une nouvelle signature « personnalisée ». Une signature est personnalisée lorsqu'elle inclut l'identifiant unique de puce (ECID, Exclusive Chip Identification), un identifiant unique propre au processeur Apple dans le cas présent, dans le cadre de la demande de signature. Seul ce processeur Apple peut utiliser la signature unique remise par le serveur. Lorsque le règlement Sécurité maximale est actif, la mémoire morte d'amorçage et le LLB contribuent à vérifier qu'une signature donnée n'est pas seulement signée par Apple, mais qu'elle est également signée pour le Mac en question, ce qui lie essentiellement cette version de macOS à ce Mac en particulier.

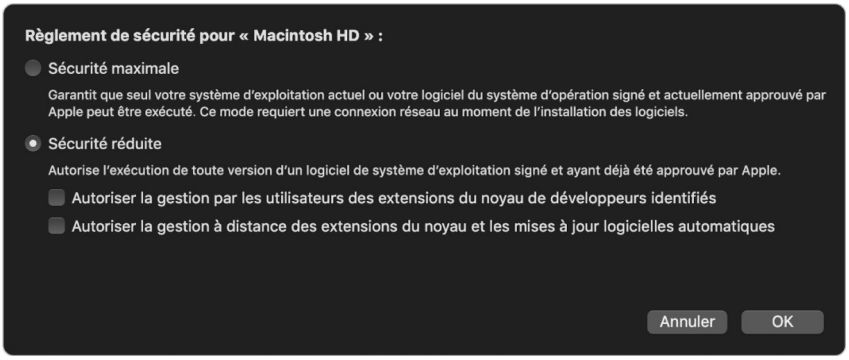
Sélection du règlement Sécurité maximale de macOS.

L’utilisation d’un serveur de signature en ligne fournit également une meilleure protection contre les attaques par retour en arrière par rapport aux signatures globales habituelles. Dans un système de signature globale, l’époque de sécurité pourrait avoir reculé plusieurs fois, mais un système qui n’a jamais vu les programmes internes les plus récents ne le saura pas. Par exemple, un ordinateur qui se croit actuellement à l’époque de sécurité 1 accepte un logiciel provenant de l’époque 2, même s’il se trouve en fait à l’époque 5. Avec le système de signature en ligne de la puce Apple, le serveur de signature peut rejeter la création de signatures pour un logiciel qui n’appartient pas à l’époque de sécurité la plus récente.

De plus, si un assaillant découvre une faille après un changement d’époque de sécurité, il ne peut pas simplement récupérer le logiciel vulnérable d’une époque précédente sur le système A pour l’appliquer au système B afin de l’attaquer. Le fait que le logiciel vulnérable d’une époque antérieure a été personnalisé pour le système A contribue à le rendre non transférable, donc il ne peut pas être utilisé contre le système B. Tous ces mécanismes fonctionnent ensemble pour mieux garantir que les assaillants ne peuvent pas installer un logiciel vulnérable sur un Mac afin de contourner les protections apportées par la plus récente version du logiciel. Cependant, un utilisateur qui a en sa possession le nom d’utilisateur et le mot de passe d’un administrateur pour le Mac peut choisir le règlement de sécurité qui convient à ses besoins.

Règlement Sécurité réduite

Le règlement Sécurité réduite se comporte de façon semblable au règlement Sécurité normale d’un Mac avec processeur Intel et puce T2, où un fournisseur (Apple, dans le cas présent) génère pour le code une signature numérique confirmant qu’il en est à l’origine. Ce comportement contribue à empêcher les assaillants d’insérer un code non signé. Apple qualifie cette signature de « globale », car elle est utilisable pour une durée indéterminée sur n’importe quel Mac réglé sur Sécurité réduite. Le règlement Sécurité réduite ne fournit aucune protection contre les attaques par retour en arrière (bien que les modifications non autorisées du système d’exploitation puissent rendre les données utilisateur inaccessibles). Pour en savoir plus, consultez la section Extensions de noyau sur un Mac avec puce Apple.



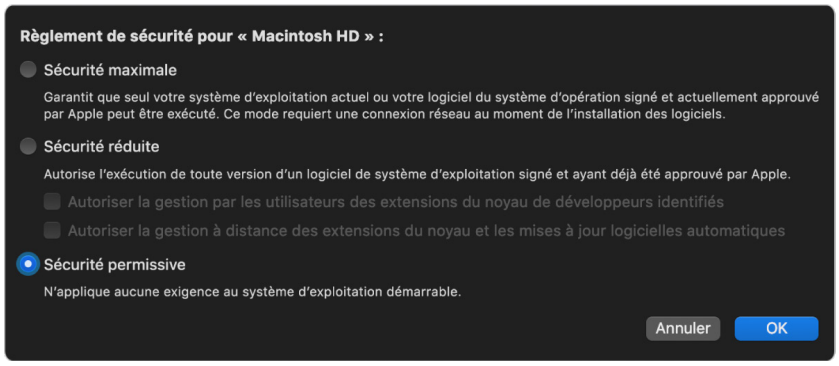
Sélection du règlement Sécurité réduite de macOS.

En plus de permettre aux utilisateurs d'exécuter des versions antérieures de macOS, le règlement Sécurité réduite est requis pour d'autres actions susceptibles de mettre en danger la sécurité du système de l'utilisateur, comme l'introduction d'extensions de noyau (kexts) tierces. Les extensions de noyau bénéficient des mêmes privilèges que le noyau. Par conséquent, toute vulnérabilité d'une extension de noyau tierce est susceptible de mettre en danger le système d'exploitation dans son ensemble. C'est pourquoi les développeurs sont fortement encouragés à adopter les extensions système, et ce, avant la fin de la prise en charge des extensions de noyau par macOS et les futurs ordinateurs Mac dotés d'une puce Apple. Même lorsque les extensions de noyau tierces sont activées, elles ne peuvent pas être chargées dans le noyau sur demande. Au lieu de cela, elles sont ajoutées à une collection du noyau auxiliaire (AuxKC) dont le hachage est stocké dans le fichier LocalPolicy et qui, par conséquent, requiert un redémarrage. Pour en savoir plus sur la génération d'une AuxKC, consultez la section Extensions de noyau sous macOS.

Règlement Sécurité permissive

Le règlement Sécurité permissive est destiné aux utilisateurs qui acceptent le risque de soumettre leur Mac à un état considérablement moins sécurisé. Ce mode est différent du mode « Aucune sécurité » d'un Mac avec processeur Intel et puce T2. Grâce au règlement Sécurité permissive, la validation des signatures est tout de même effectuée tout au long de la chaîne de démarrage sécurisé, mais le fait de régler le règlement à « Sécurité permissive » ordonne à iBoot d'accepter les objets de démarrage signés localement par le Secure Enclave, comme une collection du noyau de démarrage généré par l'utilisateur et conçu à partir d'un noyau XNU personnalisé. Ainsi, le règlement Sécurité permissive permet aussi à l'architecture d'exécuter un noyau arbitraire « Système d'exploitation nullement approuvé ». Lorsqu'une collection du noyau de démarrage personnalisée ou un système d'exploitation nullement approuvé est chargé sur le système, certaines clés de déchiffrement deviennent inaccessibles afin d'empêcher tout système d'exploitation nullement approuvé d'accéder aux données des systèmes d'exploitation de confiance.

Important : Apple ne fournit et ne prend en charge aucun noyau XNU personnalisé.



Sélection du règlement Sécurité permissive de macOS.

Le règlement Sécurité permissive diffère en un autre point du réglage Aucune sécurité d'un Mac avec processeur Intel et puce T2 : il s'agit d'une condition préalable pour effectuer certaines rétrogradations de sécurité qui étaient auparavant contrôlables de manière indépendante. Tout particulièrement, l'utilisateur doit reconnaître qu'il règle le système à Sécurité permissive pour désactiver la protection de l'intégrité du système sur un Mac avec puce Apple. Cela est nécessaire parce que la désactivation de la protection de l'intégrité du système a toujours rendu le noyau plus vulnérable. En particulier, la désactivation de la protection de l'intégrité du système sur un Mac avec puce Apple désactive l'obligation de signature des extensions de noyau lors de la génération de l'AuxKC, ce qui permet le chargement de toute extension de noyau arbitraire dans la mémoire du noyau. Une autre amélioration a été apportée à la protection de l'intégrité du système sur un Mac avec puce Apple en retirant les règlements de la mémoire vive non volatile et en les plaçant dans le fichier LocalPolicy. Ainsi, la désactivation de la protection de l'intégrité du système requiert l'authentification d'un utilisateur ayant accès à la clé de signature du fichier LocalPolicy à partir de recoveryOS (en maintenant le bouton d'alimentation enfoncé). Il est ainsi beaucoup plus difficile pour un logiciel malveillant, voire pour un assaillant physiquement présent, de désactiver la protection de l'intégrité du système.

Il n'est pas possible de rétrograder le règlement de sécurité à Sécurité permissive à partir de l'utilitaire Sécurité au démarrage. L'utilisateur peut procéder à la rétrogradation uniquement à partir de Terminal dans recoveryOS, à l'aide d'outils de ligne de commande comme `csrutil` (pour désactiver la protection de l'intégrité du système). Après que l'utilisateur a procédé à la rétrogradation, la rétrogradation en question est signalée par l'utilitaire Sécurité au démarrage pour permettre à l'utilisateur de facilement régler la sécurité à un règlement plus sécurisé.

Remarque : Un Mac avec puce Apple ne requiert ni ne prend en charge aucune règle de démarrage sur support particulière, car tous les démarrages sont techniquement effectués localement. Si un utilisateur choisit de démarrer à partir d'un support externe, cette version du système d'exploitation doit d'abord être personnalisée au moyen d'un redémarrage authentifié à partir de recoveryOS. Ce redémarrage a pour effet de créer un fichier LocalPolicy sur le disque interne utilisé pour effectuer un démarrage de confiance à partir du système d'exploitation stocké sur le support externe. Cela signifie que la configuration du démarrage à partir du support externe est toujours explicitement activée pour chaque système d'exploitation et requiert dès lors l'autorisation de l'utilisateur. Par conséquent, aucune configuration sécurisée supplémentaire n'est nécessaire.

Création et gestion de la clé de signature du fichier LocalPolicy

Création

Lors de la première installation de macOS à l'usine, ou lors d'une installation connectée après formatage, le Mac exécute du code à partir du disque virtuel de restauration temporaire pour initialiser les réglages par défaut. Pendant ce processus, l'environnement de restauration crée une nouvelle paire de clés publique et privée qui est contenue dans le Secure Enclave. La clé privée est connue sous le nom de *OIK (Owner Identity Key, clé d'identité du propriétaire)*. Si une OIK existe déjà, elle est détruite par ce processus. L'environnement de restauration initialise également la clé utilisée pour le verrouillage d'activation, connue sous le nom d'*UIK (User Identity Key, clé d'identité de l'utilisateur)*. Une partie de ce processus est propre au Mac avec puce Apple : lorsque la certification de l'UIK est demandée pour le verrouillage d'activation, un ensemble de contraintes à appliquer au moment de la validation sur le fichier LocalPolicy est inclus. Si l'appareil n'arrive pas à faire certifier une UIK pour le verrouillage d'activation (par exemple parce que l'appareil est déjà associé à un compte Localiser mon Mac et signalé comme perdu), il ne peut pas procéder à la création d'un fichier LocalPolicy. Si un appareil reçoit un *ucrt (User identity Certificate, certificat d'identité de l'utilisateur)*, celui-ci contient des contraintes de règlement imposées par le serveur et des contraintes de règlement demandées par l'utilisateur dans une extension X.509 v3.

Lorsque le verrouillage d'activation ou un ucrt est récupéré, il est stocké dans une base de données sur le serveur en plus d'être renvoyé à l'appareil. Une fois que l'appareil détient un ucrt, une demande de certification pour la clé publique qui correspond à l'OIK est envoyée au serveur *BAA (Basic Attestation Authority, autorité d'attestation de base)*. Le serveur BAA vérifie la demande de certification de l'OIK à l'aide de la clé publique provenant du ucrt stocké dans la base de données à laquelle il a accès. S'il peut vérifier la certification, il certifie la clé publique, puis renvoie le *certificat d'identité du propriétaire (OIC, Owner Identity Certificate)* signé par lui-même, qui contient les contraintes stockées dans l'ucrt. L'OIC est renvoyé au Secure Enclave. Par la suite, dès que le Secure Enclave signe un nouveau fichier LocalPolicy, il attache l'OIC au manifeste Image4. Le LLB fait automatiquement confiance au certificat racine du serveur BAA. Pour cette raison, il fait confiance à l'OIC et donc aussi à la signature du fichier LocalPolicy en général.

Contraintes RemotePolicy

Tous les fichiers Image4 (pas seulement les fichiers LocalPolicy) contiennent des contraintes pour l'évaluation des manifestes Image4. Ces contraintes sont encodées au moyen d'identifiants d'objet (OID, Object Identifiers) spéciaux dans le certificat feuille. La bibliothèque de vérification Image4 recherche l'OID spécial d'un certificat pendant l'évaluation de la signature, puis elle évalue mécaniquement les contraintes qui y sont indiquées. Les contraintes adoptent les formes suivantes :

- X must exist (X doit exister)
- X must not exist (X ne doit pas exister)
- X must have a specific value (X doit avoir une valeur précise)

Donc, par exemple, pour les signatures personnalisées, les contraintes de certificat comporteront « ECID must exist » (ECID doit exister), et pour les signatures « globales », elles comporteront « ECID must not exist » (ECID ne doit pas exister). Ces contraintes visent à garantir que tous les fichiers Image4 signés par une clé donnée doivent satisfaire à certaines exigences pour éviter la génération de manifestes Image4 signés erronés.

Dans le contexte de chaque fichier LocalPolicy, ces contraintes de certificat Image4 sont connues sous le nom de *RemotePolicy*. Un élément RemotePolicy différent peut exister pour les fichiers LocalPolicy de différents environnements de démarrage. L'élément RemotePolicy est utilisé pour restreindre le fichier LocalPolicy de recoveryOS de sorte que recoveryOS, lorsqu'il démarre, peut uniquement se comporter comme s'il appliquait le règlement Sécurité maximale. Cela augmente la confiance dans l'intégrité de l'environnement de démarrage de recoveryOS comme le lieu où le règlement de sécurité peut être modifié. L'élément RemotePolicy empêche le fichier LocalPolicy de contenir l'ECID du Mac qui l'a généré ainsi que le hachage du nonce des règles distantes (`rpnh`) précis qui est stocké dans le composant de stockage sécurisé de ce Mac. Le `rpnh` et par conséquent l'élément RemotePolicy ne changent que lorsque des opérations relatives à Localiser mon Mac et au verrouillage d'activation sont effectuées, par exemple des inscriptions, des désinscriptions, des verrouillages à distance et des effacements à distance. Les contraintes des règles distantes sont déterminées et précisées au moment de la certification de l'UIK, puis elles sont signées dans l'ucrt émis. Certaines contraintes des règles distantes, comme l'ECID, le ChipID et le BoardID, sont déterminées par le serveur pour empêcher un appareil de signer les fichiers LocalPolicy pour un autre appareil. D'autres contraintes des règles distantes peuvent être spécifiées par l'appareil pour contribuer à empêcher une rétrogradation de sécurité du fichier LocalPolicy sans la présentation de l'authentification locale requise pour accéder à l'OIK actuel et de l'authentification à distance du compte pour lequel le verrouillage d'activation de l'appareil est activé.

Contenu d'un fichier LocalPolicy d'un Mac avec puce Apple

LocalPolicy est un fichier Image4 signé par le Secure Enclave. Image4 est un format de structure de données ASN.1 (Abstract Syntax Notation One) avec encodage DER qui est utilisé pour décrire les informations qui se rapportent aux objets de la chaîne de démarrage sécurisé sur les plateformes Apple. Dans un modèle de démarrage sécurisé qui repose sur Image4, les règlements de sécurité sont requis au moment de l'installation du logiciel amorcée par une demande de signature soumise à un serveur central de signature d'Apple. Si le règlement est accepté, le serveur de signature renvoie un fichier Image4 signé, qui contient des séquences de codes de quatre caractères (FourCC). Ces fichiers Image4 signés et ces séquences FourCC sont évalués lors du démarrage par des logiciels tels que la mémoire morte d'amorçage et le LLB.

Transmission de la propriété entre systèmes d'exploitation

L'accès à l'OIK (Owner Identity Key, clé d'identité du propriétaire) est appelé « propriété ». La propriété est requise pour autoriser les utilisateurs à resigner le fichier LocalPolicy après la modification de règlements ou de logiciels. L'OIK est protégée par la même hiérarchie de clés que celle décrite dans la section Protection scellée des clés (SKP) : l'OIK est protégée par la même clé de chiffrement des clés (KEK) que la clé de chiffrement du volume (VEK). Cela signifie qu'elle est habituellement protégée autant par les mots de passe de l'utilisateur que par les mesures du système d'exploitation et du règlement. Il n'existe qu'une seule OIK pour tous les systèmes d'exploitation du Mac. Par conséquent, lors de l'installation d'un deuxième système d'exploitation, le consentement explicite des utilisateurs du premier système d'exploitation est requis pour transmettre la propriété aux utilisateurs du deuxième. Cependant, aucun utilisateur n'existe pour le deuxième système d'exploitation lors de l'exécution du programme d'installation à partir du premier système d'exploitation. Les utilisateurs des systèmes d'exploitation ne sont habituellement pas générés avant le démarrage du système d'exploitation et l'exécution d'Assistant réglages. Deux nouvelles actions sont donc requises lors de l'installation d'un deuxième système d'exploitation sur un Mac avec puce Apple :

- la création d'un fichier LocalPolicy pour le deuxième système d'exploitation;
- la préparation d'un « utilisateur d'installation » pour transmettre la propriété.

Lors de l'exécution de l'assistant d'installation pour effectuer une installation sur un volume secondaire vide, une invite demande à l'utilisateur s'il souhaite copier un utilisateur du volume actuel pour en faire le premier utilisateur du deuxième volume. Si l'utilisateur accepte, l'utilisateur d'installation créé est en réalité une KEK dérivée des clés de mot de passe et de matériel de l'utilisateur sélectionné, qui est ensuite utilisée pour chiffrer l'OIK lors de sa transmission au deuxième système d'exploitation. Ensuite, à partir de l'assistant d'installation du deuxième système d'exploitation, la saisie du mot de passe de cet utilisateur est requise pour permettre l'accès à l'OIK dans le Secure Enclave pour le nouveau système d'exploitation. Si les utilisateurs choisissent de ne pas copier un utilisateur, l'utilisateur d'installation est quand même créé de la même façon, mais un mot de passe vide est utilisé plutôt que celui d'un utilisateur. Ce deuxième processus existe pour certains scénarios d'administration du système. Toutefois, les utilisateurs qui veulent effectuer des installations sur plusieurs volumes et transmettre la propriété de la façon la plus sécurisée possible devraient toujours choisir de copier un utilisateur du premier au deuxième système d'exploitation.

LocalPolicy sur un Mac avec puce Apple

Pour un Mac avec puce Apple, le contrôle local du règlement de sécurité a été délégué à une application qui s'exécute dans le Secure Enclave. Ce logiciel peut utiliser les informations d'identification de l'utilisateur ainsi que le mode de démarrage du processeur principal pour déterminer qui peut modifier le règlement de sécurité et à partir de quel environnement de démarrage. Cela contribue à empêcher les logiciels malveillants d'utiliser les commandes du règlement de sécurité contre l'utilisateur en les rétrogradant pour obtenir plus de privilèges.

Propriétés du manifeste LocalPolicy

Le fichier LocalPolicy contient des codes architecturaux FourCC qui se trouvent dans presque tous les fichiers Image4, tels que BORD (qui désigne l'identifiant d'une carte ou d'un modèle), CHIP (qui désigne une puce Apple précise) ou l'identifiant unique de puce (ECID). Mais les codes FourCC présentés plus bas traitent uniquement des règlements de sécurité configurables par les utilisateurs.

Remarque : Apple utilise le terme *One True recoveryOS (1TR)* pour se référer à un démarrage du système recoveryOS principal effectué en appuyant sur le bouton d'alimentation. Ce démarrage est différent d'un démarrage normal de recoveryOS, qui peut être effectué au moyen de la NVRAM ou peut se produire lorsque des erreurs surviennent au démarrage. L'utilisation du bouton d'alimentation signifie qu'il y a peu de risque que l'environnement de démarrage soit accessible par un assaillant qui se serait introduit dans macOS par des moyens logiciels.

Hachage du nonce LocalPolicy (lpnh)

- *Type :* OctetString (48)
- *Environnements mutables :* 1TR, recoveryOS, macOS
- *Description :* Le `lpnh` sert à protéger le fichier LocalPolicy contre les rejeux. Il s'agit d'un hachage SHA384 du LPN (LocalPolicy Nonce, nonce du fichier LocalPolicy), qui est stocké dans le composant de stockage sécurisé et qui est accessible au moyen de la mémoire morte d'amorçage du Secure Enclave ou du Secure Enclave lui-même. Le nonce brut n'est jamais lisible par le processeur d'application et n'est lisible que par sepOS. Un assaillant qui tenterait de convaincre le LLB de la validité du fichier LocalPolicy antérieur dont il se serait emparé serait contraint de placer dans le composant de stockage sécurisé une valeur dont le hachage correspondrait au même `lpnh` que celui trouvé dans le fichier LocalPolicy qu'il souhaiterait réexécuter. Normalement, il n'y a qu'un LPN valide dans le système, excepté lors des mises à jour logicielles pendant lesquelles deux LPN sont simultanément valides, et ce, pour permettre à l'utilisateur de lancer l'ancien logiciel en cas d'erreur de mise à jour. Toute modification d'un fichier LocalPolicy de n'importe quel système d'exploitation entraîne une nouvelle signature de tous les règlements avec la nouvelle valeur *lpnh*, qui correspond au nouveau LPN trouvé dans le composant de stockage sécurisé. Cette modification se produit lorsque l'utilisateur modifie les réglages de sécurité ou crée de nouveaux systèmes d'exploitation avec un nouveau fichier LocalPolicy pour chacun d'eux.

Hachage du nonce des règles distantes (rpnh)

- *Type :* OctetString (48)
- *Environnements mutables :* 1TR, recoveryOS, macOS
- *Description :* Le `rpnh` se comporte de façon identique au `lpnh`, mais il n'est mis à jour que lorsque les règles distantes sont mises à jour, par exemple lors de la modification de l'état d'inscription à Localiser. Cette modification se produit lorsque l'utilisateur modifie l'état de Localiser sur son Mac.

Hachage du nonce de recoveryOS (ronh)

- *Type :* OctetString (48)
- *Environnements mutables :* 1TR, recoveryOS, macOS

- *Description :* Le `ronh` se comporte de façon identique au `lpnh`, mais on le retrouve uniquement dans le fichier LocalPolicy de recoveryOS. Il est mis à jour lorsque recoveryOS est mis à jour, comme lors de mises à jour logicielles. Un nonce séparé du `lpnh` et du `rpnh` est utilisé de sorte que lorsqu'un appareil est désactivé au moyen de Localiser, les systèmes d'exploitation existants peuvent être désactivés (en supprimant leur LPN et leur RPN du composant de stockage sécurisé) sans empêcher le démarrage de recoveryOS. Ainsi, les systèmes d'exploitation peuvent être réactivés lorsque le propriétaire prouve son contrôle sur le système en saisissant son mot de passe iCloud utilisé pour le compte Localiser. Cette modification se produit lorsqu'un utilisateur met à jour recoveryOS ou crée de nouveaux systèmes d'exploitation.

Hachage du manifeste Image4 de l'étape suivante (nsih)

- *Type :* OctetString (48)
- *Environnements mutables :* 1TR, recoveryOS, macOS
- *Description :* Le champ *nsih* représente un hachage SHA384 de la structure de données du manifeste Image4 qui décrit le système macOS démarré. Le manifeste Image4 de macOS contient des mesures pour tous les objets de démarrage, tels qu'iBoot, le cache statique de confiance, l'arborescence de l'appareil, la collection du noyau de démarrage et le hachage racine du volume système signé (VSS). Lorsque le LLB reçoit l'ordre de démarrer un système macOS donné, il est conçu pour vérifier que le hachage du manifeste Image4 de macOS joint à iBoot correspond à la valeur enregistrée dans le champ `nsih` du fichier LocalPolicy. De cette manière, le `nsih` capture l'intention de l'utilisateur quant au système d'exploitation pour lequel l'utilisateur a créé un fichier LocalPolicy. Les utilisateurs modifient la valeur `nsih` de façon implicite lorsqu'ils effectuent une mise à jour logicielle.

Hachage du règlement de l'AuxKC (auxp)

- *Type :* OctetString (48)
- *Environnements mutables :* macOS
- *Description :* L'`auxp` est un hachage SHA384 du règlement UAKL (User-Authorized Kext List, liste d'extensions de noyau autorisées par l'utilisateur). Il est utilisé au moment de la génération d'une AuxKC pour veiller à ce que seules les extensions de noyau autorisées par l'utilisateur soient incluses dans l'AuxKC. `smb2` est une condition préalable pour configurer ce champ. Les utilisateurs modifient implicitement la valeur `auxp` lorsqu'ils modifient l'UAKL en approuvant une extension de noyau dans Préférences Système > Sécurité et confidentialité.

Hachage du manifeste Image4 de l'AuxKC (auxi)

- *Type :* OctetString (48)
- *Environnements mutables :* macOS

- *Description :* Après que le système a vérifié que le hachage de l'UAKL correspond à la valeur du champ auxp du fichier LocalPolicy, il demande à l'application du processeur Secure Enclave chargée des signatures du fichier LocalPolicy de signer l'AuxKC. Ensuite, un hachage SHA384 de la signature du manifeste Image4 de l'AuxKC est stocké dans le fichier LocalPolicy pour éviter le risque de mélanger les AuxKC signées antérieurement et de les faire correspondre à un système d'exploitation au moment du démarrage. Si iBoot trouve le champ `auxi` dans le fichier LocalPolicy, il essaie de charger l'AuxKC à partir du stockage et valide sa signature. Il vérifie aussi que le hachage du manifeste Image4 joint à l'AuxKC correspond à la valeur du champ `auxi`. Si pour une raison quelconque le chargement de l'AuxKC échoue, le système poursuit son démarrage sans cet objet de démarrage et sans qu'aucune extension de noyau tierce ne soit chargée. Le champ auxp est une condition préalable à la configuration du champ auxi du fichier LocalPolicy. Les utilisateurs modifient implicitement la valeur `auxi` lorsqu'ils modifient l'UAKL en approuvant une extension de noyau dans Préférences Système > Sécurité et confidentialité.

Hachage du reçu de l'AuxKC (auxr)

- *Type :* OctetString (48)
- *Environnements mutables :* macOS
- *Description :* L'`auxr` est un hachage SHA384 du reçu de l'AuxKC qui indique l'ensemble exact d'extensions de noyau comprises dans l'AuxKC. Le reçu de l'AuxKC est un sous-ensemble de l'UAKL, car les extensions de noyau peuvent être exclues de l'AuxKC même si elles sont autorisées par l'utilisateur lorsqu'elles sont réputées être le vecteur d'attaques. Par ailleurs, certaines extensions de noyau susceptibles d'être utilisées pour outrepasser la limite utilisateur-noyau peuvent occasionner une perte de fonctionnalité, telle que l'incapacité d'utiliser Apple Pay ou de visionner du contenu 4K et HDR. Les utilisateurs qui souhaitent utiliser ces fonctionnalités doivent opter pour une inclusion de l'AuxKC plus restrictive. Le champ auxp est une condition préalable à la configuration du champ `auxr` du fichier LocalPolicy. Les utilisateurs modifient implicitement la valeur `auxr` lorsqu'ils créent une nouvelle AuxKC dans Préférences Système > Sécurité et confidentialité.

Hachage du manifeste Image4 de CustomOS (coih)

- *Type :* OctetString (48)
- *Environnements mutables :* 1TR
- *Description :* Le `coih` est un hachage SHA384 du manifeste Image4 de CustomOS. L'entité de ce manifeste est utilisée par iBoot (à la place du noyau XNU) pour transférer le contrôle. Les utilisateurs modifient la valeur `coih` de façon implicite lorsqu'ils utilisent l'outil de ligne de commande `kmutil configure–boot` dans 1TR.

IDUU du groupe de volumes APFS (vuid)

- *Type :* OctetString (16)
- *Environnements mutables :* 1TR, recoveryOS, macOS
- *Description :* Le `vuid` indique le groupe de volumes que le noyau doit utiliser comme racine. Ce champ est principalement informatif et n'est pas utilisé pour appliquer des contraintes de sécurité. Ce champ `vuid` est configuré implicitement par l'utilisateur lors de la création de l'installation d'un système d'exploitation.

IDUU du groupe de la clé de chiffrement de clés (kuid)

- *Type :* OctetString (16)
- *Environnements mutables :* 1TR, recoveryOS, macOS
- *Description :* Le `kuid` indique le volume démarré. La clé de chiffrement des clés a généralement été utilisée à des fins de protection des données. Pour chaque fichier LocalPolicy, le kuid est utilisé pour protéger la clé de signature du fichier LocalPolicy. Le champ `kuid` est configuré implicitement par l'utilisateur lors de la création de l'installation d'un système d'exploitation.

Mesure de la règle de démarrage de confiance de couplage de recoveryOS (prot)

- *Type :* OctetString (48)
- *Environnements mutables :* 1TR, recoveryOS, macOS
- *Description :* Une mesure de la règle de démarrage de confiance (TBPM, Trusted Boot Policy Measurement) de couplage de recoveryOS est un calcul spécial, par itération, de hachage SHA384 appliqué au manifeste Image4 du fichier LocalPolicy, à l'exception des nonces, afin de fournir une valeur cohérente dans le temps (car les nonces tels que le `lpnh` sont actualisés fréquemment). Le champ prot, qu'on trouve uniquement dans le fichier LocalPolicy de chaque instance de macOS, fournit une valeur de couplage qui indique quel fichier LocalPolicy de recoveryOS correspond au fichier LocalPolicy de macOS. Le champ `prot` se trouve uniquement dans le fichier LocalPolicy de chaque instance de macOS et fournit une valeur de couplage qui indique quel fichier LocalPolicy de recoveryOS correspond au fichier LocalPolicy de macOS.

Présence d'un fichier LocalPolicy de recoveryOS signé par le Secure Enclave (hrlp)

- *Type :* Booléenne
- *Environnements mutables :* 1TR, recoveryOS, macOS
- *Description :* Le champ `hrlp` indique si la valeur `prot` ci-dessus est la mesure d'un fichier LocalPolicy de recoveryOS signé par le Secure Enclave. Si ce n'est pas le cas, le fichier LocalPolicy de recoveryOS est signé par le serveur de signature en ligne d'Apple, qui signe des éléments comme les fichiers Image4 de macOS.

Multidémarrage sécurisé (smb0)

- *Type :* Booléenne
- *Environnements mutables :* 1TR, recoveryOS
- *Description :* Si la valeur `smb0` est présente et vérifiée, le LLB autorise la signature globale du manifeste Image4 de l'étape suivante au lieu d'exiger une signature personnalisée. Les utilisateurs peuvent modifier ce champ au moyen de l'utilitaire Sécurité au démarrage ou de `bputil` pour rétrograder le règlement de sécurité à Sécurité réduite.

Multidémarrage sécurisé (smb1)

- *Type :* Booléenne
- *Environnements mutables :* 1TR

- *Description :* Si la valeur `smb1` est présente et vérifiée, iBoot autorise les objets tels que la collection du noyau personnalisé à être signés par le Secure Enclave avec la clé qui a signé le fichier LocalPolicy. La présence de la valeur `smb0` est une condition préalable de la présence de la valeur `smb1`. Ce champ peut être modifié par les utilisateurs au moyen d'outils de ligne de commande tels que `csrutil` ou `bputil` pour rétrograder le règlement de sécurité à Sécurité permissive.

Multidémarrage sécurisé (smb2)

- *Type :* Booléenne
- *Environnements mutables :* 1TR
- *Description :* Si la valeur `smb2` est présente et vérifiée, iBoot autorise la collection du noyau auxiliaire à être signée par le Secure Enclave avec la clé qui a signé le fichier LocalPolicy. La présence de la valeur `smb0` est une condition préalable de la présence de la valeur `smb2`. Ce champ peut être modifié par les utilisateurs au moyen de l'utilitaire Sécurité au démarrage ou de `bputil` pour rétrograder le règlement de sécurité à Sécurité réduite et activer les extensions de noyau tierces.

Multidémarrage sécurisé (smb3)

- *Type :* Booléenne
- *Environnements mutables :* 1TR
- *Description :* Si la valeur `smb3` est présente et vérifiée, cela signifie qu'un utilisateur de l'appareil a confié le contrôle de son système à une solution de gestion des appareils mobiles (GAM). La présence de ce champ fait en sorte que l'application du processeur Secure Enclave qui contrôle le fichier LocalPolicy accepte les authentifications de la solution de GAM au lieu d'exiger l'authentification locale de l'utilisateur. Ce champ peut être modifié par les utilisateurs au moyen de l'utilitaire Sécurité au démarrage ou de `bputil` pour permettre le contrôle géré des extensions de noyau tierces et des mises à jour logicielles. (Sous macOS 11.2 et les versions ultérieures, la GAM peut également lancer une mise à jour vers la version de macOS la plus récente si le mode de sécurité est réglé à Sécurité maximale.)

Multidémarrage sécurisé (smb4)

- *Type :* Booléenne
- *Environnements mutables :* recoveryOS, macOS
- *Description :* Si la valeur `smb4` est présente et vérifiée, cela signifie que l'appareil a confié le contrôle du système d'exploitation à la solution de GAM au moyen d'Apple School Manager ou d'Apple Business Manager. La présence de ce champ fait en sorte que l'application du processeur Secure Enclave qui contrôle le fichier LocalPolicy accepte les authentifications de la solution de GAM au lieu d'exiger l'authentification locale de l'utilisateur. Ce champ est modifié par la solution de GAM lorsque le numéro de série d'un appareil apparaît dans Apple School Manager ou Apple Business Manager.

Protection de l'intégrité du système (sip0)

- *Type :* Entier non signé de 64 bits
- *Environnements mutables :* 1TR

- *Description :* La valeur `sip0` comporte les bits du règlement de protection de l'intégrité du système qui étaient précédemment stockés dans la NVRAM. Les nouveaux bits du règlement de protection de l'intégrité du système sont ajoutés ici (plutôt que d'utiliser les champs du fichier LocalPolicy comme les champs suivants) s'ils sont utilisés uniquement dans macOS, et non par le LLB. Ce champ peut être modifié par les utilisateurs au moyen de `csrutil` à partir de 1TR pour désactiver la protection de l'intégrité du système et rétrograder le règlement de sécurité à Sécurité permissive.

Protection de l'intégrité du système (sip1)

- *Type :* Booléenne
- *Environnements mutables :* 1TR
- *Description :* Si la valeur `sip1` est présente et vérifiée, iBoot autorisera les échecs de validation du hachage racine du VSS. Ce champ peut être modifié par les utilisateurs avec `csrutil` ou `bputil` à partir de 1TR.

Protection de l'intégrité du système (sip2)

- *Type :* Booléenne
- *Environnements mutables :* 1TR
- *Description :* Si la valeur sip2 est présente et vérifiée, iBoot ne verrouillera pas le registre interne *CTRR (Configurable Text Read-only Region, région configurable de lecture seule du texte)* qui marque la mémoire du noyau comme n'étant pas inscriptible. Ce champ peut être modifié par les utilisateurs avec `csrutil` ou `bputil` à partir de 1TR.

Protection de l'intégrité du système (sip3)

- *Type :* Booléenne
- *Environnements mutables :* 1TR
- *Description :* Si la valeur `sip3` est présente et vérifiée, iBoot n'appliquera pas sa liste d'autorisation intégrée pour la variable des arguments de démarrage de la mémoire vive non volatile, ce qui aurait pour effet de filtrer les options transmises au noyau. Ce champ peut être modifié par les utilisateurs avec `csrutil` ou `bputil` à partir de 1TR.

Certificats et élément RemotePolicy

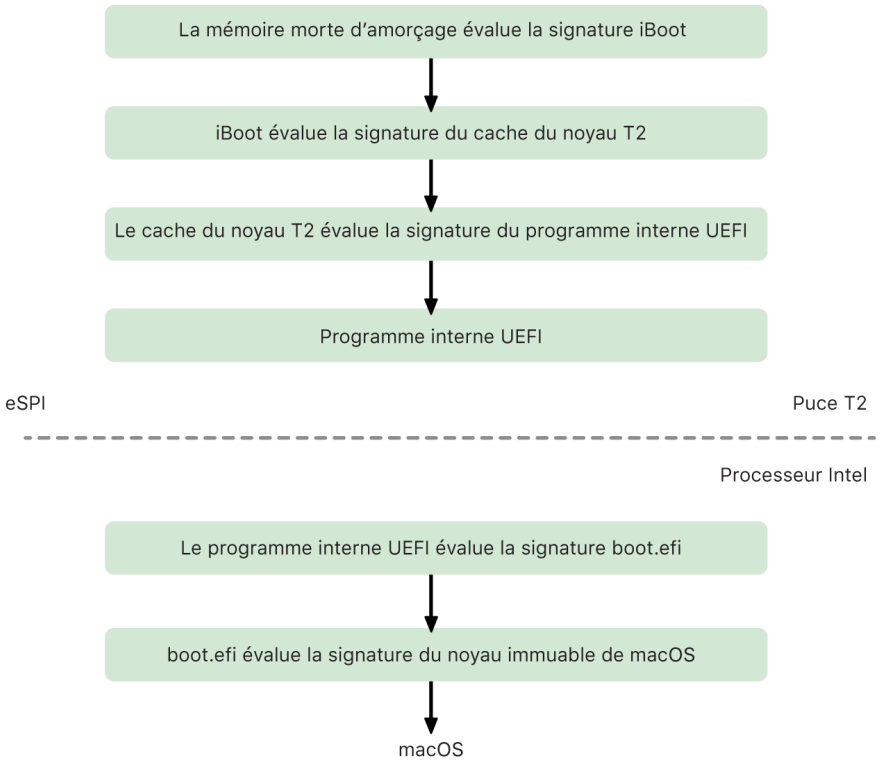
Conformément à la description donnée dans la section Création et gestion de la clé de signature du fichier LocalPolicy, le manifeste Image4 du fichier LocalPolicy contient également l'OIC (Owner Identity Certificate, certificat d'identité du propriétaire) et l'élément RemotePolicy intégré.

Ordinateurs Mac avec processeur Intel

Processus de démarrage d’un Mac avec processeur Intel

Mac avec processeur Intel et puce T2 Security d’Apple

Lorsqu’un ordinateur Mac avec processeur Intel et puce T2 Security d’Apple est allumé, la puce effectue un démarrage sécurisé à partir de sa mémoire morte d’amorçage tout comme sur iPhone, iPad et les Mac avec puce Apple. Ce processus valide le chargeur de démarrage iBoot. Il s’agit de la première étape de la chaîne de confiance. iBoot vérifie le code du noyau et de l’extension du noyau sur la puce T2, qui vérifie ensuite le programme interne Intel UEFI. Celui-ci ainsi que la signature associée sont d’abord accessibles uniquement par la puce T2.



Chaîne de démarrage sécurisé T2 de macOS.

Après vérification, l’image du programme interne UEFI est associée à une partie de la mémoire de la puce T2. Cette mémoire est mise à la disposition du processeur Intel par le bus d’interface périphérique série améliorée (eSPI). Lorsque le processeur Intel démarre, il récupère le programme interne UEFI par l’eSPI à partir de la copie du programme interne associée à la mémoire dont l’intégrité a été vérifiée qui se trouve sur la puce T2.

L’évaluation de la chaîne de confiance se poursuit sur le processeur Intel : le programme interne UEFI évalue la signature pour boot.efi, qui est le chargeur d’amorçage de macOS. Les signatures de démarrage sécurisé macOS logées dans le processeur Intel sont stockées dans le même format Image4 que celui du démarrage sécurisé d’iOS, d’iPadOS et de la puce T2, et le code qui analyse les fichiers Image4 est le même que le code durci de l’implémentation de démarrage sécurisé actuelle d’iOS et d’iPadOS. Boot.efi vérifie ensuite la signature d’un nouveau fichier appelé immutablekernel. Lorsque le démarrage sécurisé est activé, le fichier immutablekernel représente l’ensemble complet des extensions du noyau Apple requises pour démarrer macOS. La règle de démarrage sécurisé prend fin avec le passage au fichier immutablekernel, puis les règlements de sécurité macOS (comme la protection de l’intégrité du système et les extensions du noyau) prennent effet.

En cas d’erreur ou d’échec de ce processus, le Mac lance le mode de récupération, le mode de récupération de la puce T2 Security d’Apple ou le mode DFU (Device Firmware Upgrade, mise à niveau du programme interne de l’appareil) de la puce T2 Security d’Apple.

Microsoft Windows sur un Mac avec processeur Intel et puce T2

Par défaut, un Mac avec processeur Intel qui prend en charge le démarrage sécurisé ne fait confiance qu’au contenu signé par Apple. Cependant, pour améliorer la sécurité des installations Boot Camp, Apple prend également en charge le démarrage sécurisé de Windows. Le programme interne UEFI comprend une copie de l’autorité de certification « Microsoft Windows Production CA 2011 » utilisée pour authentifier les chargeurs d’amorçage Microsoft.

Remarque : Aucune confiance n’est actuellement accordée à l’autorité de certification « Microsoft Corporation UEFI CA 2011 », qui permettrait la vérification du code signé par les partenaires de Microsoft. Cette autorité de certification est couramment utilisée pour vérifier l’authenticité des chargeurs d’amorçage d’autres systèmes d’exploitation comme les variantes de Linux.

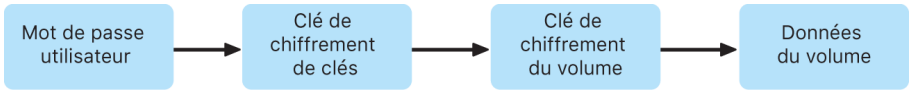
La prise en charge du démarrage sécurisé de Windows n’est pas activée par défaut. Elle est plutôt activée à l’aide d’Assistant Boot Camp. Lorsqu’un utilisateur lance Assistant Boot Camp, macOS est reconfiguré pour faire confiance au code signé directement par Microsoft. Une fois qu’Assistant Boot Camp a terminé la configuration, si macOS échoue à l’évaluation de confiance directe d’Apple pendant le démarrage sécurisé, le programme interne UEFI tente d’évaluer le degré de confiance de l’objet selon le formatage du démarrage sécurisé UEFI. Si l’évaluation de confiance réussit, le Mac poursuit le démarrage de Windows. Sinon, le Mac démarre recoveryOS et informe l’utilisateur de l’échec de l’évaluation de confiance.

Ordinateurs Mac avec processeur Intel sans puce T2

Un ordinateur Mac avec processeur Intel sans puce T2 ne prend pas en charge le démarrage sécurisé. Par conséquent, le programme interne UEFI charge le démarreur macOS (boot.efi) à partir du système de fichiers sans vérification, puis le démarreur charge le noyau (prelinkedkernel) à partir du système de fichiers sans vérification. Afin de protéger l’intégrité de la chaîne de démarrage, les utilisateurs devraient activer les mécanismes de sécurité suivants :

- *Protection de l’intégrité du système (SIP) :* Activée par défaut, cette option protège le démarreur et le noyau contre des écritures malveillantes depuis l’intérieur d’un macOS actif.

- *FileVault :* Cette fonction peut être activée de deux façons : par l'utilisateur ou par un administrateur de la gestion des appareils mobiles (GAM). Elle assure une protection contre un assaillant physiquement présent qui utiliserait le mode disque cible pour remplacer le démarreur.
- *Mot de passe du programme interne :* Cette fonction peut être activée de deux façons : par l'utilisateur ou par un administrateur de la GAM. Elle veille à empêcher un assaillant physiquement présent de lancer d'autres modes de démarrage, comme recoveryOS, le mode Utilisateur unique ou le mode disque cible, à partir desquels il pourrait remplacer le démarreur. Elle contribue également à prévenir le démarrage à partir d'autres supports que l'assaillant pourrait utiliser pour exécuter un code et ainsi remplacer le démarreur.



Processus de déverrouillage d'un Mac avec processeur Intel sans puce T2.

Modes de démarrage d'un Mac avec processeur Intel et puce T2 Security d'Apple

Un ordinateur Mac avec processeur Intel et puce T2 Security d'Apple dispose de différents modes de démarrage pouvant être lancés au démarrage en appuyant sur des combinaisons de touches reconnues par le programme interne UEFI ou par le démarreur. Certains modes de démarrage, comme le mode Utilisateur unique, ne fonctionneront pas à moins que le règlement de sécurité soit réglé à Aucune sécurité dans l'utilitaire Sécurité au démarrage.

Mode	Combinaison de touches	Description
Démarrage de macOS	Aucune	Le programme interne UEFI cède le contrôle au démarreur de mac OS (une application UEFI), qui le cède au noyau macOS. Lors du démarrage standard d'un Mac sur lequel FileVault est activé, le démarreur macOS présente l'interface Fenêtre de connexion, qui prend le mot de passe pour déchiffrer le stockage.
Gestionnaire de démarrage	Option ( )	Le programme interne UEFI lance l'application UEFI intégrée, qui présente à l'utilisateur une interface de sélection du disque de démarrage.
Mode disque cible (TDM)	T	Le programme interne UEFI lance l'application UEFI intégrée, qui expose le dispositif de stockage interne en tant que dispositif de stockage primaire à base de blocs par connexion Fire Wire, Thunderbolt, USB ou une combinaison des trois (selon le modèle Mac).

Mode	Combinaison de touches	Description
Mode Utilisateur unique	Commande ( ) + S	Le noyau macOS passe l'indicateur –s dans le vecteur d'argument de launchd, puis launchd crée la coquille logicielle d'utilisateur unique dans le téléscripteur de l'app Console. *Remarque :* Si l'utilisateur quitte la coquille, macOS poursuit son démarrage jusqu'à la fenêtre de connexion.
recoveryOS	Commande ( ) + R	Le programme interne UEFI charge une version minimale de macOS à partir d'un fichier signé de l'image disque (.dmg) sur le dispositif de stockage interne.
recoveryOS sur Internet	Option ( ) + Commande ( ) + R	L'image disque signée est téléchargée à partir d'Internet par HTTP.
Diagnostic	D	Le programme interne UEFI charge un environnement de diagnostic UEFI minimal à partir d'un fichier signé de l'image disque sur le dispositif de stockage interne.
Diagnostic sur Internet	Option ( ) + D	L'image disque signée est téléchargée à partir d'Internet par HTTP.
Démarrage de Windows	Aucune	Si Windows a été installé avec Boot Camp, le programme interne UEFI cède le contrôle au démarreur Windows, qui le cède au noyau Windows.

Utilitaire Sécurité au démarrage sur un Mac doté d’une puce T2 Security d’Apple

Aperçu

Sur un Mac avec processeur Intel et puce T2 Security d’Apple, l’utilitaire Sécurité au démarrage traite certains réglages du règlement de sécurité. L’utilitaire est accessible en démarrant recoveryOS et en sélectionnant l’utilitaire Sécurité au démarrage à partir du menu Utilitaires. Il protège les réglages de sécurité pris en charge des manipulations faciles d’un assaillant.

Capture d’écran de l’utilitaire Sécurité au démarrage.

L’authentification est requise pour toute modification importante du règlement, même en mode de récupération. À l’ouverture initiale de l’utilitaire Sécurité au démarrage, celui-ci demande à l’utilisateur de saisir le mot de passe administrateur de l’installation primaire de macOS qui est associé à l’instance de recoveryOS en cours d’exécution. S’il n’y a pas d’administrateur, il faut en créer un pour pouvoir modifier le règlement. De plus, la puce T2 requiert que le Mac soit en train d’exécuter recoveryOS et qu’une authentification avec des informations d’identification appuyées par le Secure Enclave ait lieu avant que toute modification puisse être apportée au règlement. Deux exigences implicites régissent la modification du règlement de sécurité. recoveryOS doit :

- démarrer à partir d’un dispositif de stockage connecté directement à la puce T2, car les partitions sur d’autres appareils ne possèdent pas d’informations d’identification appuyées par le Secure Enclave et associées au dispositif de stockage interne;
- se trouver sur un volume APFS, car il ne prend en charge que le stockage de l’authentification dans les informations d’identification de récupération envoyées au Secure Enclave sur le volume de prédémarrage APFS d’un disque. Le démarrage sécurisé n’est pas compatible avec les volumes de format HFS+.

Ce règlement est uniquement affiché dans l'utilitaire Sécurité au démarrage sur les ordinateurs Mac avec processeur Intel et puce T2. Même si la plupart des cas d'usage ne devraient pas nécessiter la modification de la règle de démarrage sécurisé, les utilisateurs ont le dernier mot quant aux réglages de l'appareil et peuvent choisir, en fonction de leurs besoins, de désactiver ou de rétrograder la fonctionnalité de démarrage sécurisé de leur Mac.

Les modifications apportées à la règle de démarrage sécurisé depuis cette app ne s'appliquent qu'à l'évaluation de la chaîne de confiance vérifiée sur le processeur Intel. L'option « Démarrage sécurisé de la puce T2 » n'est jamais désactivée.

La règle de démarrage sécurisé propose les trois options suivantes : Sécurité maximale, Sécurité normale et Aucune sécurité. La règle Aucune sécurité désactive complètement l'évaluation du démarrage sécurisé sur le processeur Intel et permet à l'utilisateur de démarrer ce qu'il veut.

Règle de démarrage Sécurité maximale

Sécurité maximale est la règle de démarrage par défaut. Elle se comporte de façon semblable à iOS, à iPadOS ou à Sécurité maximale sur un Mac avec puce Apple. Au moment où le logiciel est téléchargé et son installation est en cours de préparation, il est personnalisé au moyen d'une signature qui inclut l'identifiant unique de puce (ECID, Exclusive Chip Identification), un identifiant unique propre à la puce T2 dans le cas présent, dans le cadre de la demande de signature. Seule cette puce T2 peut utiliser la signature unique remise par le serveur. Lorsque la règle Sécurité maximale est active, le programme interne UEFI est conçu pour vérifier qu'une signature donnée n'est pas seulement signée par Apple, mais qu'elle est également signée pour le Mac en question, ce qui lie essentiellement cette version de macOS à ce Mac en particulier. Cela contribue à prévenir les attaques par retour en arrière décrites à la section qui traite de la sécurité maximale sur un Mac avec puce Apple.

Règle de démarrage Sécurité normale

La règle de démarrage Sécurité normale ressemble un peu au démarrage sécurisé UEFI traditionnel, où un fournisseur (Apple, dans le cas présent) génère pour le code une signature numérique confirmant qu'il en est à l'origine. Les assaillants sont ainsi incapables d'insérer un code non signé. Apple qualifie cette signature de « globale », car elle est utilisable pour une durée indéterminée sur n'importe quel Mac réglé sur Sécurité normale. Ni iOS, ni iPadOS, ni la puce T2 ne prennent en charge les signatures globales. Cette règle ne prévient pas les attaques par retour en arrière.

Règle de démarrage sur support

La règle de démarrage sur support existe uniquement sur un ordinateur Mac avec processeur Intel et puce T2 et est indépendante de la règle de démarrage sécurisé. Ainsi, même si un utilisateur désactive le démarrage sécurisé, le comportement par défaut qui empêche le démarrage du Mac à partir de tout autre support que le dispositif de stockage directement connecté à la puce T2 demeure inchangé. (La règle de démarrage sur support n'est pas requise sur les Mac avec puce Apple.) Pour en savoir plus, consultez la section Contrôle du règlement de sécurité du disque de démarrage.

Protection par mot de passe du programme interne sur un Mac avec processeur Intel

macOS sur les ordinateurs Mac avec processeur Intel et puce T2 Security d'Apple prend en charge l'utilisation d'un mot de passe de programme interne pour contribuer à empêcher la modification involontaire des réglages du programme interne sur un Mac donné. L'utilisation d'un mot de passe de programme interne est conçue pour empêcher la sélection d'autres modes de démarrage tels que recoveryOS ou le mode Utilisateur unique, le démarrage à partir d'un volume non autorisé ou le mode disque cible.

Remarque : Le mot de passe du programme interne n'est pas requis sur un Mac avec puce Apple, car la fonctionnalité visée du programme interne a été placée dans recoveryOS, et (lorsque FileVault est activé) ce dernier requiert l'authentification de l'utilisateur pour autoriser l'accès à ses fonctionnalités essentielles.

Le mode le plus élémentaire de protection par mot de passe de programme interne peut être activé dans l'utilitaire de mot de passe de programme interne de recoveryOS sur un ordinateur Mac avec processeur Intel *sans* puce T2, et dans l'utilitaire Sécurité au démarrage sur un Mac avec processeur Intel *et* puce T2. Des options avancées (comme l'activation de la demande du mot de passe à chaque démarrage) sont accessibles via l'outil de ligne de commande `firmwarepasswd` sous macOS.

La configuration d'un mot de passe de programme interne est particulièrement importante pour réduire le risque d'attaques contre les ordinateurs Mac avec processeur Intel sans puce T2 par un assaillant physiquement présent. Le mot de passe du programme interne peut aider à empêcher un assaillant de démarrer recoveryOS, où il serait autrement en mesure de désactiver la protection de l'intégrité du système. La restriction du démarrage à partir d'autres supports empêche un assaillant d'exécuter un code privilégié d'un autre système d'exploitation dans le but d'attaquer les programmes internes périphériques.

Un mécanisme de réinitialisation du mot de passe du programme interne vient en aide aux utilisateurs qui oublient leur mot de passe. Il suffit d'appuyer sur une combinaison de touches au démarrage pour obtenir une chaîne propre au modèle à fournir à AppleCare. AppleCare signe numériquement une ressource dont la signature est vérifiée par l'identifiant de ressource uniforme (URI). Si la signature est validée et que le contenu vise le Mac en question, le programme interne UEFI supprime le mot de passe du programme interne.

Pour les utilisateurs qui ne veulent pas que quelqu'un d'autre puisse supprimer le mot de passe du programme interne par des moyens logiciels, l'option `–disable–reset–capability` a été ajoutée à l'outil de ligne de commande `firmwarepasswd` sous macOS 10.15. Avant d'activer cette option, l'utilisateur doit comprendre que s'il oublie son mot de passe, il devra assumer les coûts du remplacement de la carte logique, qui sera alors nécessaire pour supprimer le mot de passe. Les organisations qui veulent protéger leurs ordinateurs Mac contre les assaillants externes et les employés doivent régler un mot de passe de programme interne sur les systèmes dont ils sont propriétaires. Cela peut être accompli sur l'appareil de l'une des façons suivantes :

- manuellement au moment de l'approvisionnement, en utilisant l'outil de ligne de commande `firmwarepasswd`;
- à l'aide d'outils de gestion tiers qui utilisent l'outil de ligne de commande `firmwarepasswd`;
- à l'aide de la solution de gestion des appareils mobiles (GAM).

Environnements de diagnostic et recoveryOS d'un Mac avec processeur Intel

recoveryOS

La partition de récupération recoveryOS est entièrement séparée de la partition macOS principale, et le contenu est entièrement stocké dans un fichier d'image disque nommé BaseSystem.dmg. Une liste de blocs BaseSystem.chunklist associée est également utilisée pour vérifier l'intégrité du fichier BaseSystem.dmg. La liste de blocs est une série de hachages pour des blocs de 10 Mo du fichier BaseSystem.dmg. Le programme interne UEFI évalue la signature de la liste de blocs avant d'évaluer le hachage d'un bloc du fichier BaseSystem.dmg à la fois, ce qui veille à garantir qu'il corresponde au contenu signé figurant dans la liste. Si la correspondance ne peut être établie pour un de ces hachages, le démarrage à partir de la partition locale de recoveryOS est abandonné, et le programme interne UEFI tente plutôt de démarrer à partir recoveryOS sur Internet.

Si la vérification est un succès, le programme interne UEFI monte le fichier BaseSystem.dmg en tant que disque virtuel et lance le fichier boot.efi qu'il contient. Le programme interne UEFI n'a pas à vérifier le fichier boot.efi, et celui-ci n'a pas à vérifier le noyau, car l'intégrité du contenu complet du système d'exploitation (dont ces éléments sont un sous-ensemble) a déjà été vérifiée.

Diagnostic Apple

La procédure de démarrage de l'environnement de diagnostic local est presque la même que pour le lancement de recoveryOS. Des fichiers distincts AppleDiagnostics.dmg et AppleDiagnostics.chunklist sont utilisés, mais ils sont vérifiés de la même façon que les fichiers BaseSystem. Plutôt que de lancer boot.efi, le programme interne UEFI lance un fichier à l'intérieur de l'image disque (fichier .dmg) nommé diags.efi, qui appelle ensuite divers autres pilotes UEFI pouvant interfacer avec le matériel et vérifier la présence d'erreurs.

Environnement de diagnostic et recoveryOS sur Internet

Si une erreur est survenue lors du lancement de l'environnement de récupération ou de diagnostic local, le programme interne UEFI tente plutôt de télécharger les images à partir d'Internet. (Un utilisateur peut également demander spécifiquement la récupération des images par Internet en appuyant sur des séquences de touches particulières au démarrage.) La validation de l'intégrité des images disques et des listes de blocs téléchargées auprès du serveur de récupération du système d'exploitation est effectuée de la même façon que pour les images récupérées à partir d'un dispositif de stockage.

Bien que la connexion au serveur de récupération du système d'exploitation soit établie par HTTP, l'intégrité du contenu téléchargé complet est vérifiée de la façon mentionnée ci-dessus. Par conséquent, celui-ci est protégé contre toute manipulation par un assaillant ayant pris le contrôle du réseau. Si la procédure de vérification de l'intégrité échoue pour l'un des blocs, la demande auprès du serveur de récupération du système d'exploitation est répétée 11 fois avant son abandon et l'affichage d'une erreur.

Lorsque les modes de récupération et de diagnostic par Internet ont été ajoutés aux ordinateurs Mac en 2011, on a convenu qu'il valait mieux utiliser le transport HTTP et traiter les authentifications du contenu au moyen d'un mécanisme de liste de blocs, plutôt que d'implémenter HTTPS, un protocole plus complexe, dans le programme interne UEFI, et donc d'augmenter la surface d'attaque du programme interne.

Mises à jour logicielles sécurisées

Aperçu

La sécurité est un processus. Il n'est pas suffisant de démarrer de manière fiable la version du système d'exploitation installée à l'usine. Un mécanisme pour obtenir rapidement et sécuritairement les dernières mises à jour de sécurité est également nécessaire. Apple propose régulièrement des mises à jour logicielles pour résoudre les problèmes de sécurité émergents. Les utilisateurs d'appareils iOS et iPadOS reçoivent des notifications de mises à jour sur l'appareil. Les mises à jour de macOS sont disponibles dans Préférences Système. Les mises à jour se font sans fil, ce qui favorise l'adoption rapide des plus récents correctifs de sécurité.

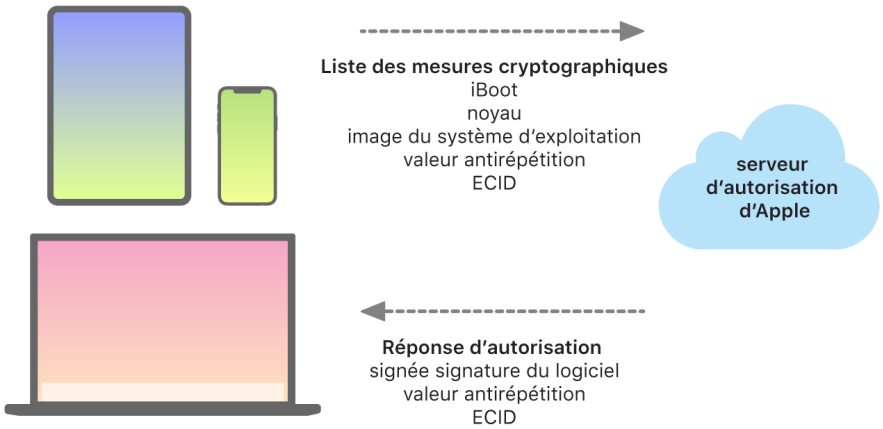
Le processus de mise à jour utilise la même base matérielle sécurisée que le démarrage sécurisé pour autoriser uniquement l'installation de code signé par Apple. Il utilise également le processus d'autorisation du logiciel système pour vérifier que seules les copies des versions du système d'exploitation activement signées par Apple peuvent être installées sur les appareils iOS et iPadOS, ou les ordinateurs Mac dont la règle de démarrage sécurisé de l'utilitaire Sécurité au démarrage est réglée à Sécurité maximale. Grâce à la mise en place de ces processus sécuritaires, Apple peut arrêter de signer des versions plus anciennes du système d'exploitation qui comportent des failles et ainsi prévenir les attaques par retour en arrière.

Pour augmenter la sécurité des mises à jour logicielles, une copie intégrale d'iOS ou d'iPadOS est téléchargée et installée lorsqu'un appareil est connecté par câble à un Mac. Pour les mises à jour du logiciel effectuées par connexion sans fil, *seuls les composants nécessaires à la mise à jour sont téléchargés*, au lieu de l'intégralité du système d'exploitation, ce qui améliore l'efficacité du réseau. Par ailleurs, les mises à jour logicielles peuvent être mises en cache sur un Mac doté de macOS 10.13 ou d'une version ultérieure (avec la mise en cache de contenu activée), afin que les appareils iOS et iPadOS n'aient pas à télécharger de nouveau la mise à jour nécessaire sur Internet. Ils n'ont alors qu'à communiquer avec les serveurs d'Apple pour conclure le processus de mise à jour.

Processus de mise à jour personnalisé

Lors d'une mise à niveau ou d'une mise à jour, une connexion est établie avec le serveur d'Apple chargé d'autoriser l'installation, qui envoie une liste de mesures cryptographiques pour chaque paquet à installer (par exemple iBoot, le noyau et l'image du système d'exploitation), une valeur antirejeu aléatoire (le nonce) et l'identifiant unique de la puce (ECID).

Le serveur d’autorisation compare alors la liste de mesures qui lui est fournie aux versions dont l’installation est autorisée et, s’il trouve une correspondance, ajoute l’ECID à la mesure et signe le résultat. Le serveur transmet un jeu complet de données signées à l’appareil dans le cadre du processus de mise à niveau. L’ajout de l’ECID « personnalise » l’autorisation pour l’appareil émetteur de la requête. En accordant son autorisation et sa signature uniquement pour des mesures connues, le serveur veille à garantir que la mise à jour se déroule exactement comme prévu par Apple.



Interaction des appareils Apple avec le serveur d’autorisation d’Apple.

L’évaluation de la chaîne de confiance au démarrage vérifie que la signature provient bien d’Apple et que la mesure de l’élément chargé à partir du dispositif de stockage, combinée à l’ECID, correspond à ce que couvre la signature. Ces étapes visent à garantir que, sur les appareils qui prennent en charge la personnalisation, l’autorisation est propre à un appareil et qu’une ancienne version du système d’exploitation ou du programme interne ne peut pas être copiée sur un autre appareil. Le nonce contribue à empêcher un assaillant d’enregistrer la réponse du serveur et de l’utiliser pour altérer un appareil ou modifier d’une quelconque façon le logiciel système.

Le processus de personnalisation est la raison pour laquelle une connexion réseau à Apple est systématiquement requise pour mettre à jour tout appareil doté d’une puce Apple, y compris un Mac avec processeur Intel et puce T2 Security d’Apple.

Enfin, le volume de données utilisateur n’est jamais monté au cours d’une mise à jour logicielle afin d’empêcher toute opération de lecture ou d’écriture sur ce volume pendant les mises à jour.

Sur les appareils dotés du Secure Enclave, ce dernier fait également appel à l’autorisation du logiciel système pour vérifier l’intégrité de son logiciel et il est conçu pour empêcher l’installation d’une version antérieure.

Intégrité du système d’exploitation

Apple conçoit ses systèmes d’exploitation autour de la sécurité, avec une base matérielle sécurisée, qui assure la sécurité du démarrage, et un processus de mise à jour logicielle sécurisé sûr et rapide. Les systèmes d’exploitation d’Apple utilisent aussi les capacités du matériel (puces) spécialement conçu pour empêcher toute utilisation malveillante pendant le fonctionnement du système. Ces fonctionnalités protègent l’intégrité du code vérifié pendant son exécution. En résumé, le système d’exploitation d’Apple contribue à parer les exploits et les attaques, que ceux-ci proviennent d’apps malveillantes, du Web ou d’un autre canal. Les protections énumérées dans la présente section sont disponibles sur les appareils dotés d’un système sur une puce d’Apple compatible, c’est-à-dire les appareils iOS, iPadOS, tvOS, watchOS et maintenant les Mac avec puce Apple dotés de macOS.

Fonctionnalité	A10	A11, S3	A12, S4	A13, S5	A14, S6	M1
Protection de l’intégrité du noyau	✓	✓	✓	✓	✓	✓
Restrictions d’autorisation rapide		✓	✓	✓	✓	✓
Protection de l’intégrité du coprocesseur système			✓	✓	✓	✓
Codes			✓	✓	✓	✓
Couche de protection de page		✓	✓	✓	✓	Voir la remarque ci-dessous.

Remarque : La couche de protection de page (PPL) exige que la plateforme exécute *uniquement* du code signé et de confiance. Ce modèle de sécurité ne s’applique pas à macOS.

Protection de l’intégrité du noyau

Après l’initialisation du noyau du système d’exploitation, la protection de l’intégrité du noyau (KIP) est activée pour contribuer à empêcher la modification du code du noyau et des pilotes. Le contrôleur de mémoire fournit une zone de mémoire physique protégée qu’iBoot utilise pour charger le noyau et les extensions de noyau. Après le démarrage, le contrôleur de mémoire refuse l’écriture sur la zone de mémoire physique protégée. L’unité de gestion de la mémoire (UGM) du processeur d’application est configurée de manière à aider à prévenir la mise en correspondance du code privilégié de la mémoire physique à l’extérieur de la zone de mémoire protégée et la mise en correspondance microprogrammable de la mémoire physique à l’intérieur de la zone de mémoire du noyau.

Pour empêcher la reconfiguration, le matériel utilisé pour activer la KIP est verrouillé après le processus de démarrage.

Restrictions d’autorisation rapide

Les systèmes sur une puce A11 Bionic, S3 et de génération ultérieure d’Apple comportent une nouvelle primitive matérielle. Cette primitive, les restrictions d’autorisation rapides, comprend un registre de processeur qui restreint rapidement les autorisations par fil d’exécution. Grâce à ces restrictions d’autorisation rapide (aussi connues sous le nom de registres APRR), les systèmes d’exploitation compatibles peuvent supprimer les autorisations d’exécution de la mémoire sans subir le coût d’un appel système et de la consultation ou purge de la table de pages. Ces registres fournissent un niveau supplémentaire d’atténuation des attaques provenant du Web, particulièrement pour le code compilé à l’exécution (« à la volée »), car il est impossible d’exécuter efficacement la mémoire en même temps que sa lecture et son écriture.

Protection de l’intégrité du coprocesseur système

Le programme interne du coprocesseur gère de nombreuses tâches système essentielles, comme le Secure Enclave, le processeur de capteur d’image et le coprocesseur de mouvement. Par conséquent, sa sécurité est un élément essentiel de la sécurité de l’ensemble du système. Pour prévenir les modifications du programme interne du coprocesseur, Apple utilise le mécanisme *SCIP (System Coprocessor Integrity Protection, protection de l’intégrité du coprocesseur système)*.

La SCIP utilise un mécanisme semblable à celui de la protection de l’intégrité du noyau (KIP, Kernel Integrity Protection). Au démarrage, iBoot charge chaque programme interne du coprocesseur dans une zone de mémoire protégée, réservée et séparée de la zone de KIP. iBoot configure chaque unité de la mémoire du coprocesseur de manière à contribuer à prévenir :

- les mises en correspondance exécutables à l’extérieur de sa section de la zone de mémoire protégée;
- les mises en correspondance microprogrammables à l’intérieur de sa section de la zone de mémoire protégée.

Toujours au démarrage, c’est le système d’exploitation du Secure Enclave qui est utilisé pour configurer la SCIP propre à ce coprocesseur. Après le processus de démarrage, le matériel utilisé pour activer la SCIP est verrouillé afin d’empêcher la reconfiguration.

Codes d’authentification des pointeurs

Les codes d’authentification des pointeurs (PAC) sont utilisés pour empêcher l’exploitation des bogues de corruption de mémoire. Les logiciels système et les apps intégrées utilisent les PAC pour contribuer à prévenir la modification des pointeurs de fonctions et des adresses de retour (pointeurs de code). Les PAC utilisent cinq valeurs secrètes 128 bits pour signer les instructions du noyau et les données. Chaque processus de l’espace utilisateur possède ses propres clés B. Les éléments sont salés et signés comme suit.

Élément	Clé	Sel
Adresse de retour des fonctions	IB	Adresse de stockage
Pointeurs de fonctions	IA	0
Fonction d’appel de blocs	IA	Adresse de stockage

Élément	Clé	Sel
Cache de méthode Objective-C	IB	Adresse de stockage + classe + sélecteur
Entrées de la table des méthodes virtuelles C++	IA	Adresse de stockage + hachage (nom de méthode mutilé)
Étiquette « aller à » calculée	IA	Hachage (nom de fonction)
État du fil d'exécution du noyau	GA	•
Registres d'état du fil d'exécution utilisateur	IA	Adresse de stockage
Pointeurs de la table des méthodes virtuelles C++	DA	0

La valeur de signature est stockée dans les bits de remplissage inutilisés dans le haut du pointeur 64 bits. La signature est vérifiée avant son utilisation, et le remplissage est réinitialisé pour contribuer à garantir le fonctionnement de l'adresse de pointeur. Si cette vérification échoue, l'opération est annulée. Cette vérification rend de nombreuses attaques plus difficiles, par exemple les attaques par programmation orientée retour (ROP, Return-Oriented Programming), qui consistent à manipuler les adresses de retour des fonctions stockées sur la pile pour amener l'appareil à exécuter du code existant.

Couche de protection de page

La couche de protection de page (PPL) sous iOS, iPadOS et watchOS est conçue pour empêcher la modification du code de l'espace utilisateur une fois sa signature vérifiée. Tirant parti de la protection de l'intégrité du noyau et des restrictions d'autorisation rapide, la PPL gère le remplacement des autorisations de la table de pages afin de garantir qu'elle seule puisse modifier les pages protégées qui contiennent un code utilisateur et des tables de pages. Ce système réduit considérablement la surface d'attaque en favorisant le respect de l'intégrité du code à l'échelle du système, même si le noyau est compromis. Cette protection n'est pas offerte sous macOS, car la PPL ne s'applique qu'aux systèmes qui exigent la signature de l'intégralité du code exécuté.

Fonctionnalités de sécurité du système supplémentaires sous macOS

Fonctionnalités de sécurité du système supplémentaires sous macOS

macOS fonctionne avec un ensemble plus large de composants matériels (par exemple des processeurs Intel, des processeurs Intel associés à une puce T2 Security d'Apple et des systèmes sur une puce d'Apple) et se prête à toutes sortes d'usages informatiques courants. Bien que certains utilisateurs n'utilisent que les apps de base préinstallées ou celles disponibles dans l'App Store, d'autres sont des bidouilleurs de noyau qui doivent désactiver essentiellement toutes les protections des plateformes afin de pouvoir exécuter et mettre à l'essai leur code comme s'il détenait le plus haut niveau de confiance. La plupart des utilisateurs se répartissent entre ces deux extrêmes. Un grand nombre d'entre eux utilisent des périphériques et des logiciels qui requièrent différents niveaux d'accès. Apple a conçu la plateforme macOS en adoptant une approche intégrée par rapport au matériel, aux logiciels et aux services pour en faire une plateforme avant tout sécuritaire, simple à configurer, à déployer et à gérer, mais en conservant les possibilités attendues par ses utilisateurs en matière de configuration. macOS comprend les technologies de sécurité clés dont les professionnels des TI ont besoin pour protéger les données d'entreprise et assurer l'intégration des appareils à l'environnement réseau sécurisé de l'organisation.

Les caractéristiques suivantes répondent aux différents besoins des utilisateurs de macOS et contribuent à les sécuriser. En voici la liste :

- Sécurité du volume système signé
- Protection de l'intégrité du système
- Caches de confiance
- Protection des périphériques
- Prise en charge et sécurité de Rosetta 2 (traduction automatique) pour un Mac avec puce Apple
- Prise en charge et protection de l'accès direct à la mémoire
- Prise en charge et sécurité des extensions de noyau
- Prise en charge et sécurité de la mémoire morte d'option
- Sécurité du programme interne UEFI pour les ordinateurs Mac avec processeur Intel

Sécurité du volume système signé sous macOS

Apple a introduit le volume système en lecture seule dans macOS 10.15. Il s'agit d'un volume isolé, dédié au contenu du système. macOS 11 a permis d'ajouter des protections cryptographiques robustes au contenu du système sur un *volume système signé (VSS)*. Le VSS est doté d'un mécanisme de noyau qui vérifie l'intégrité du contenu du système pendant son fonctionnement et qui rejette toute donnée, code ou autre, qui ne présente pas de signature cryptographique valide émise par Apple.

Non seulement le VSS aide à prévenir l'altération de tout logiciel Apple faisant partie du système d'exploitation, il rend aussi la mise à jour logicielle de macOS plus fiable et plus sûre. Comme le VSS utilise les instantanés du système de fichiers d'Apple (APFS), si une mise à jour ne parvient pas à être installée, la version antérieure du système peut être restaurée sans réinstallation.

Depuis son apparition, l'APFS contribue à l'intégrité des métadonnées du système de fichiers au moyen de sommes de contrôle non cryptographiques sur le dispositif de stockage interne. Le VSS consolide le mécanisme d'intégrité en ajoutant des hachages cryptographiques de manière à englober chaque octet de données de fichiers. Les données du dispositif de stockage interne (y compris les métadonnées du système de fichiers) sont hachées de façon cryptographique dans le chemin de lecture, puis le hachage est comparé à une valeur attendue dans les métadonnées du système de fichiers. En cas de différence, le système considère que les données ont été altérées et ne les renvoient pas au logiciel qui les a demandées.

Chaque hachage SHA256 du VSS est stocké dans l'arborescence principale des métadonnées du système de fichiers, qui est elle-même hachée. De plus, comme chaque nœud de l'arbre vérifie récursivement l'intégrité des hachages de ses fichiers dépendants, une méthode semblable à l'arbre de hachage (ou arbre de Merkle) binaire, la valeur de hachage du nœud racine, appelée *sceau*, couvre donc chaque octet de données du VSS. Par conséquent, la signature cryptographique couvre l'intégralité du volume système.

Lors de l'installation et des mises à jour de macOS, ce sceau est recalculé à partir du système de fichiers directement sur l'appareil, et cette mesure est comparée à celle qu'Apple a signée. Sur un Mac avec puce Apple, le chargeur de démarrage vérifie le sceau avant de transmettre le contrôle au noyau. Sur un Mac avec processeur Intel et puce T2 Security d'Apple, le chargeur de démarrage renvoie la mesure et la signature au noyau, qui vérifie directement le sceau avant de monter le système de fichiers racine. Dans les deux cas, si la vérification échoue, le processus de démarrage s'arrête, et l'utilisateur est invité à réinstaller macOS.

Cette procédure est répétée à chaque démarrage à moins que l'utilisateur ait choisi un règlement de sécurité inférieur et qu'il ait explicitement choisi de désactiver le volume système signé.

VSS et signature du code

La signature du code a toujours lieu et est imposée par le noyau. Le volume système signé offre sa protection lorsque tout octet de données est lu à partir du dispositif de stockage interne. En revanche, la signature du code offre une protection lorsque des objets Mach sont mis en correspondance avec la mémoire en tant qu'exécutables. Le VSS et la signature du code protègent tous les deux le code exécutable sur tous les chemins de lecture et d'exécution.

VSS et FileVault

Sous macOS 11, une protection au repos équivalente pour le contenu du système est assurée par le VSS et le volume système n'a donc plus besoin d'être chiffré. Toute modification apportée au système de fichiers lorsque ce dernier est au repos sera détectée par le système de fichiers lorsqu'il procédera à leur lecture. Si l'utilisateur a activé FileVault, son contenu sur le volume de données est tout de même chiffré au moyen d'un secret fourni par lui-même.

Si l’utilisateur choisit de désactiver le VSS, le système devient vulnérable aux altérations lorsqu’il est au repos, et de telles altérations pourraient permettre à un assaillant d’extraire des données chiffrées de l’utilisateur lors du prochain démarrage du système. Par conséquent, le système n’autorisera pas l’utilisateur à désactiver le VSS si FileVault est activé. La cohérence exige que la protection au repos soit activée ou désactivée sur les deux volumes.

Sous macOS 10.15 ou une version antérieure, FileVault protège le système d’exploitation au repos en chiffrant le contenu de l’utilisateur et le contenu du système au moyen d’une clé protégée par un secret fourni par l’utilisateur. Cela empêche un assaillant ayant physiquement accès à l’appareil d’accéder au système de fichiers renfermant les logiciels système ou de le modifier.

VSS et Mac avec puce T2 Security d’Apple

Sur un Mac avec puce T2 Security d’Apple, seul macOS est protégé par le VSS. Le logiciel qui s’exécute sur la puce T2 et qui vérifie macOS est protégé par le démarrage sécurisé.

Protection de l’intégrité du système

macOS utilise les autorisations du noyau pour limiter l’accès en écriture des fichiers système essentiels au moyen de la *SIP (Systeme Integrity Protection, protection de l’intégrité du système)*. Cette fonctionnalité est indépendante et s’ajoute à la KIP (Kernel Integrity Protection, protection de l’intégrité du noyau) matérielle disponible sur un Mac avec puce Apple, qui protège contre les modifications de la mémoire du noyau. La technologie de contrôle d’accès obligatoire est utilisée à ces fins et pour assurer d’autres protections au niveau du noyau, y compris la mise en bac à sable et Data Vault.

Contrôles d’accès obligatoires

macOS fait appel aux contrôles d’accès obligatoires. Ces règlements de sécurité créés par le développeur ne peuvent être annulés, contrairement aux contrôles d’accès discrétionnaires, que l’utilisateur peut contourner à sa guise.

Invisibles pour l’utilisateur, les contrôles d’accès obligatoires sont à la base de plusieurs fonctionnalités clés, comme la mise en bac à sable, les contrôles parentaux, les préférences gérées, les extensions et la protection de l’intégrité du système.

Protection de l’intégrité du système

Grâce à la *protection de l’intégrité du système*, certains emplacements clés du système de fichiers offrent uniquement l’accès en lecture seule, ce qui contribue à empêcher les programmes malveillants d’en modifier le contenu. La protection de l’intégrité du système est un réglage propre à l’ordinateur. Elle est activée par défaut lorsqu’un utilisateur met à niveau le système d’exploitation vers OS X 10.11 ou version ultérieure. Si cette fonction est désactivée sur un Mac avec processeur Intel, toutes les partitions du dispositif de stockage matériel perdent la protection. macOS applique ce règlement de sécurité à tous les processus actifs du système, même s’ils s’exécutent dans un bac à sable ou avec des privilèges administrateur.

Caches de confiance

Le cache statique de confiance fait partie de la chaîne de démarrage sécurisé. Il s'agit d'un registre de confiance de tous les fichiers binaires Mach-O qui sont maîtrisés dans un volume système signé. Chaque Mach-O est représenté par un hachage de répertoire de code. Pour permettre une recherche efficace, ces hachages sont triés avant d'être insérés dans le cache de confiance. Le répertoire de code est le résultat de l'opération de signature effectuée par `codesign(1)`. Pour appliquer le cache de confiance, la SIP doit demeurer activée. Pour désactiver l'application du cache de confiance sur un Mac avec puce Apple, le démarrage sécurisé doit être réglé à « Sécurité permissive ».

Lorsqu'un fichier binaire est exécuté (qu'il s'agisse de générer un nouveau processus ou de mettre du code en correspondance avec un processus existant), son répertoire de code est extrait et haché. Si le hachage correspondant est détecté dans le cache de confiance, les privilèges de la plateforme seront accordés aux correspondances exécutables établies pour le fichier binaire. Autrement dit, ils pourront jouir de tout droit et s'exécuter sans qu'aucune autre vérification quant à l'authenticité de la signature ne soit requise. Cette méthode s'oppose à celle employée par les Mac avec processeur Intel, pour lesquels les privilèges de la plateforme sont transmis au contenu du système d'exploitation par le certificat Apple qui signe les fichiers binaires. (Ce certificat ne limite pas les droits dont le fichier binaire peut jouir.)

Les fichiers binaires qui ne se rapportent pas à la plateforme (par exemple du code tiers notarisé) doivent disposer de chaînes de certificats valides pour s'exécuter, et les droits dont ils peuvent jouir sont limités par le profil de signature du développeur qui lui est émis par le programme Apple pour les développeurs.

Tous les fichiers binaires inclus dans macOS sont signés par un *identifiant de plateforme*. Sur un Mac avec puce Apple, cet identifiant est utilisé pour indiquer que son hachage de répertoire de code doit être présent dans le cache de confiance pour être exécuté, et ce, même si le fichier binaire est signé par Apple. Sur un Mac avec processeur Intel, l'identifiant de plateforme est utilisé pour procéder aux révocations ciblées de fichiers binaires d'une version plus ancienne de macOS. Cette révocation ciblée contribue à empêcher l'exécution de ces fichiers sur des versions plus récentes.

Le cache statique de confiance verrouille complètement un ensemble de fichiers binaires en l'associant à une version précise de macOS. Ce comportement contribue à empêcher les fichiers binaires légitimement signés par Apple des systèmes d'exploitation plus anciens d'être introduits par un assaillant dans un système plus récent.

Code de la plateforme contenu en dehors du système d'exploitation

Apple envoie certains fichiers binaires, comme Xcode et la suite d'outils de développement, qui ne sont pas signés par un identifiant de plateforme. Malgré tout, ils sont encore autorisés à s'exécuter avec les privilèges de la plateforme sur un Mac avec puce Apple ou puce T2. Étant donné que ce logiciel de la plateforme est inclus indépendamment de macOS, il n'est pas soumis aux pratiques de révocation imposées par le cache statique de confiance.

Caches de confiance chargeables

Apple fournit certains paquets logiciels avec des *caches de confiance chargeables*. Ces caches ont la même structure de données que le cache statique de confiance. Mais, même s'il n'y a qu'un cache statique de confiance et que le verrouillage dans des intervalles en lecture seule de son contenu est garanti une fois l'initialisation anticipée du noyau terminée, les caches de confiance chargeables sont ajoutés au système en cours d'exécution.

Ces caches de confiance sont authentifiés soit par le même mécanisme qui authentifie le programme interne de démarrage (personnalisation au moyen du service de signature de confiance d'Apple), soit en tant qu'objets validés par une signature globale (sans qu'ils soient liés à un appareil particulier par leurs signatures).

Un exemple de cache de confiance personnalisé est inclus avec l'image disque utilisée pour effectuer les diagnostics de terrain sur les Mac avec puce Apple. Ce cache de confiance est personnalisé, tout comme l'image disque, et est chargé dans le noyau de l'ordinateur Mac sujet alors qu'un mode de diagnostic a démarré sur ce dernier. Le cache de confiance permet l'exécution du logiciel qui se trouve dans l'image disque avec les privilèges de la plateforme.

Un exemple de cache de confiance validé par une signature globale est inclus avec les mises à jour logicielles de macOS. Ce cache de confiance permet à une portion de code de la mise à jour logicielle (le *cerveau de mise à jour)* de s'exécuter avec les privilèges de la plateforme. Le cerveau de mise à jour accomplit toute tâche liée à l'indexation de la mise à jour logicielle que le système hôte n'est pas en mesure d'effectuer de façon cohérente sur toutes les versions.

Sécurité du processeur périphérique des ordinateurs Mac

Tous les systèmes informatiques modernes sont équipés de nombreux processeurs périphériques intégrés qui sont dédiés à des tâches telles que la mise en réseau, l'affichage graphique et la gestion d'énergie. Ces processeurs périphériques n'ont souvent qu'une seule fonction et sont bien moins puissants que le processeur principal. Les périphériques intégrés dont la sécurité est insuffisante sont une cible facile que les assaillants peuvent exploiter pour infecter le système d'exploitation de manière persistante. Après l'infection du programme interne d'un processeur périphérique, un assaillant peut viser des logiciels sur le processeur principal ou recueillir directement des données sensibles (par exemple un appareil Ethernet pourrait voir le contenu de paquets non chiffrés).

Dans la mesure du possible, Apple s'efforce de réduire le nombre de processeurs périphériques nécessaires et d'éviter les conceptions qui nécessitent un programme interne. Cependant, lorsque des processeurs indépendants fonctionnant avec leur propre programme interne sont requis, des mesures sont prises pour faire en sorte qu'une infection ne puisse pas persister sur ce processeur. Cela peut se faire en vérifiant le processeur d'une des deux façons suivantes :

- exécuter le processeur de sorte qu'il télécharge un programme interne vérifié auprès du processeur principal au démarrage;
- faire en sorte que le processeur périphérique implémente sa propre chaîne de démarrage sécurisé pour vérifier son propre programme interne à chaque démarrage du Mac.

Apple travaille avec des fournisseurs pour vérifier leurs implémentations et améliorer leurs conceptions afin d'inclure les propriétés désirées comme :

- l'assurance d'une solidité du cryptogramme minimale;
- l'assurance de la révocation robuste des programmes internes malveillants connus;
- la désactivation des interfaces de débogage;
- la signature du programme interne avec des clés cryptographiques stockées dans des modules de sécurité matériels (HSM) contrôlés par Apple.

Ces dernières années, Apple a collaboré avec quelques fournisseurs externes pour adopter les mêmes structures de données Image4, codes de vérification et infrastructures de signature utilisés par la puce Apple.

Si ni le fonctionnement sans stockage ni le stockage avec démarrage sécurisé n'est possible, la conception fait en sorte que la mise à jour du programme interne est signée de manière cryptographique et vérifiée avant la mise à jour du stockage persistant.

Rosetta 2 sur un Mac avec puce Apple

Un Mac avec puce Apple est capable d'exécuter du code compilé pour le jeu d'instructions x86_64 au moyen du mécanisme de traduction *Rosetta 2*. Deux types de traduction sont offerts : à la volée et à l'avance.

Traduction à la volée

Dans le canal de traduction à la volée (JIT, Just in Time), un objet Mach x86_64 est rapidement identifié dans le chemin d'exécution des images. Lorsque ces images ont été trouvées, le noyau transfère le contrôle à une souche de traduction Rosetta spéciale plutôt qu'à l'éditeur de liens dynamiques, `dyld(1)`. La souche de traduction traduit ensuite les pages x86_64 lors de l'exécution de l'image. Cette traduction se produit entièrement au sein du processus. Le noyau vérifie les hachages de code de chaque page x86_64 en les comparant à la signature du code jointe au fichier binaire, et ce, même en cas de défaut de page. Si un hachage ne correspond pas, le noyau applique la politique de correction appropriée pour ce processus.

Traduction à l'avance

Dans le chemin de traduction à l'avance (AOT, Ahead of Time), les fichiers binaires x86_64 sont lus à partir du stockage aux moments où la réactivité du code est considérée comme optimale par le système. Les artéfacts traduits sont écrits sur le stockage sous la forme d'un type spécial de fichier Mach-O. Ce fichier ressemble à une image exécutable, mais il est marqué de manière à indiquer qu'il s'agit du produit traduit d'une autre image.

Dans ce modèle, l'artéfact AOT extrait toutes les informations relatives à son identité de l'image exécutable x86_64 originale. Pour faire appliquer cette liaison, une entité de l'espace utilisateur privilégié signe l'artéfact de traduction au moyen d'une clé propre à l'appareil gérée par le Secure Enclave. Cette clé est remise uniquement à l'entité espace utilisateur privilégié, qui est identifiée comme telle au moyen d'un droit restreint. Le répertoire de code créé pour l'artéfact de traduction inclut le hachage du répertoire de code de l'image exécutable x86_64 originale. On appelle *signature supplémentaire* la signature apposée sur l'artéfact de traduction.

Le canal AOT commence de la même façon que le canal JIT, avec le noyau qui transfère le contrôle au moteur d'exécution de Rosetta plutôt qu'à l'éditeur de liens dynamiques, `dyld(1)`. Mais le moteur d'exécution de Rosetta envoie ensuite une requête de communication interprocessus au service système Rosetta, qui demande si une traduction AOT est disponible pour l'image exécutable actuelle. S'il en trouve une, le service Rosetta fournit à cette traduction un descripteur qui sera mis en correspondance avec le processus et exécuté. Pendant l'exécution, le noyau fait appliquer les hachages de répertoire de code de l'artéfact de traduction, qui sont authentifiés par la signature associée à la clé de signature propre à l'appareil. Les hachages de répertoire de code de l'image x86_64 originale ne sont pas impliqués dans ce processus.

Les artéfacts traduits sont stockés dans un Data Vault qui pendant l'exécution n'est accessible par aucune autre entité que le service Rosetta. Le service Rosetta gère l'accès à son cache en distribuant des descripteurs de fichier en lecture seule à des artéfacts individuels de traduction. Cela limite l'accès au cache de l'artéfact AOT. La communication interprocessus de ce service et l'empreinte subordonnée sont intentionnellement limitées pour réduire la surface d'attaque.

Si le hachage du répertoire de code de l'image x86_64 originale ne correspond pas à celui encodé dans la signature de l'artéfact de traduction AOT, ce résultat est considéré comme équivalant à une signature de code non valide, et les actions d'application appropriées sont engagées.

Si un processus distant interroge le noyau au sujet des droits ou des autres propriétés d'identité du code d'un exécutable traduit en mode AOT, les propriétés d'identité de l'image x86_64 originale sont retournées.

Contenu du cache statique de confiance

macOS 11 ou une version ultérieure inclut des fichiers binaires Mach multiarchitectures qui contiennent des tranches de code informatique x86_64 et arm64. Sur un Mac avec puce Apple, l'utilisateur peut décider d'exécuter la tranche x86_64 d'un fichier binaire système par l'intermédiaire de Rosetta (par exemple pour charger un module qui n'a aucune variante arm64 native). Pour ce faire, le cache statique de confiance compris dans macOS contient généralement trois hachages de répertoire de code par fichier Mach-O :

- le hachage du répertoire de code de la tranche arm64;
- le hachage du répertoire de code de la tranche x86_64;
- le hachage du répertoire de code de la traduction AOT de la tranche x86_64.

La procédure de traduction AOT de Rosetta est déterministe, car elle reproduit la même sortie pour toute entrée donnée, et ce, indépendamment du moment ou de l'appareil où la traduction a eu lieu.

Pendant la construction de macOS, chaque fichier Mach-O passe par le canal de traduction AOT associé à la version de macOS en cours de construction, et le hachage de répertoire de code qui en résulte est enregistré dans le cache de confiance. Pour des raisons d'efficacité, les produits traduits ne sont pas inclus avec le système d'exploitation. Ils sont reconstitués sur demande quand l'utilisateur les requiert.

Lorsqu'une image x86_64 est exécutée sur un Mac avec puce Apple, si le hachage du répertoire de code de cette image se trouve dans le cache statique de confiance, le hachage du répertoire de code de l'artéfact AOT qui en résulte doit *également* s'y trouver. De tels produits ne sont pas signés par la clé propre à l'appareil, car l'autorité de signature est enracinée dans la chaîne de démarrage sécurisé d'Apple.

Code x86_64 non signé

Un Mac avec puce Apple n'autorise pas l'exécution d'un code arm64 natif sans signature valide. Cette signature peut être aussi simple qu'une signature de code « ad hoc » (cf. `codesign(1)`) qui ne comporte aucune identité réelle dans la partie secrète d'une paire de clés asymétrique (il s'agit uniquement d'une mesure non vérifiée du fichier binaire).

Par souci de compatibilité avec le fichier binaire, le code x86_64 traduit peut s'exécuter par l'intermédiaire de Rosetta sans aucune information de signature. Aucune identité précise n'est transmise à ce code au moyen de la procédure de signature du Secure Enclave de l'appareil, et ce code s'exécute précisément avec les mêmes limites imposées au code non signé qui s'exécute sur un Mac avec processeur Intel.

Protections de l'accès direct à la mémoire des ordinateurs Mac

Afin d'atteindre un haut débit sur les interfaces haute vitesse comme PCIe, FireWire, Thunderbolt et USB, les ordinateurs doivent prendre en charge l'accès direct à la mémoire (DMA) par les périphériques. Cela signifie qu'ils doivent avoir accès en lecture et en écriture à la mémoire vive sans la mobilisation continue du processeur central. Depuis 2012, les ordinateurs Mac mettent en œuvre de nombreuses technologies pour protéger le DMA. Résultat : le meilleur ensemble de protections du DMA sur un ordinateur, et le plus complet.

Protections de l'accès direct à la mémoire d'un Mac avec puce Apple

Les systèmes sur une puce d'Apple contiennent une unité de gestion de la mémoire d'entrée/sortie (UGMES) pour chaque agent de DMA dans le système, y compris les ports PCIe et Thunderbolt. Comme chaque UGMES dispose de son propre ensemble de tables de traduction d'adresse pour traduire les demandes de DMA, les périphériques connectés par PCIe ou Thunderbolt peuvent accéder uniquement à la mémoire qui est explicitement mise en correspondance pour leur usage. Les périphériques ne peuvent pas accéder à la mémoire qui appartient à d'autres parties du système, comme le noyau ou le programme interne, ou à la mémoire assignée à d'autres périphériques. Si une UGMES détecte une tentative d'accès par un périphérique à la mémoire qui n'est pas mise en correspondance pour l'usage de ce périphérique, une panique du noyau est déclenchée.

Protections de l’accès direct à la mémoire pour les Mac avec processeur Intel

Les ordinateurs Mac dotés d’un processeur Intel et de la technologie de virtualisation Intel pour les entrées/sorties réparties (VT-d) initialisent l’UGMES, ce qui permet la remise en correspondance du DMA et la remise en correspondance en cas d’interruption très tôt dans le processus de démarrage pour réduire plusieurs classes de vulnérabilités. Le matériel de l’UGMES d’Apple démarre en appliquant une politique de rejet par défaut. Par conséquent, dès que le système est mis en marche, il bloque automatiquement les demandes de DMA qui proviennent des périphériques. Une fois qu’il est initialisé par le logiciel, l’UGMES commence à autoriser les demandes de DMA formulées par les périphériques pour qu’ils puissent accéder aux zones de la mémoire explicitement mappées pour leur utilisation.

Remarque : La remise en correspondance en cas d’interruption pour connexion PCIe n’est pas nécessaire sur un Mac avec puce Apple, car chaque UGMES traite les MSI pour ses propres périphériques.

À partir de macOS 11, tous les ordinateurs Mac dotés d’une puce T2 Security d’Apple exécutent des pilotes UEFI qui facilitent le DMA dans un environnement restreint à l’anneau de protection 3 lorsque ces pilotes sont couplés à des appareils externes. Cette propriété permet de réduire les vulnérabilités en matière de sécurité qui pourraient être exploitées lorsqu’un appareil malveillant interagit avec un pilote UEFI d’une façon inattendue lors du démarrage. En particulier, elle réduit l’impact des vulnérabilités des pilotes qui gèrent les mémoires tampons de DMA.

Extensions de noyau sous macOS

À partir de macOS 11, si les extensions de noyau tierces sont activées, elles ne peuvent pas être chargées dans le noyau sur demande. Au lieu de cela, elles sont fusionnées dans une *collection du noyau auxiliaire (AuxKC)*, qui est chargée pendant le processus de démarrage. Pour un Mac avec puce Apple, la mesure de l’AuxKC est signée dans le fichier LocalPolicy (sur les ordinateurs plus anciens, l’AuxKC réside dans le volume de données). La reconstruction de l’AuxKC requiert l’approbation de l’utilisateur et le redémarrage de macOS pour charger les modifications dans le noyau. Le démarrage sécurisé doit aussi être réglé à « Sécurité réduite ».

Important : Les extensions de noyau ne sont plus recommandées pour macOS. Puisque ces extensions mettent en danger l’intégrité et la fiabilité du système d’exploitation, Apple recommande aux utilisateurs de privilégier des solutions qui n’y ont pas recours.

Extensions de noyau sur un Mac avec puce Apple

Les extensions de noyau doivent être explicitement activées sur un Mac avec puce Apple en maintenant le bouton d’alimentation enfoncé au démarrage pour lancer le mode 1TR (One True Recovery), en rétrogradant ensuite le règlement de sécurité à « Sécurité réduite », puis en cochant la case qui permet d’activer les extensions de noyau. Cette action requiert aussi d’entrer un mot de passe administrateur pour autoriser la rétrogradation. La combinaison du mode 1TR et de l’exigence d’un mot de passe complique les attaques purement logicielles à partir de macOS visant à introduire des extensions de noyau pour permettre à un assaillant de s’arroger les privilèges du noyau.

Une fois qu'un utilisateur autorise le chargement d'extensions de noyau, le processus de chargement des extensions de noyau approuvées par l'utilisateur est utilisé pour autoriser l'installation des extensions de noyau. L'autorisation utilisée pour ce processus est également utilisée pour capturer un hachage SHA384 de l'UAKL (User Authorized Kext List, liste d'extensions de noyau autorisées par l'utilisateur) dans le fichier LocalPolicy. Le démon de gestion du noyau (`kmd`) est ensuite chargé de valider uniquement les extensions de noyau répertoriées dans l'UAKL en vue de leur inclusion dans l'AuxKC.

- Si la protection de l'intégrité du système (SIP) est activée, la signature de chaque extension de noyau est vérifiée avant d'être incluse dans l'AuxKC.
- Si la SIP est désactivée, la signature de l'extension de noyau n'est pas imposée.

Les flux de sécurité permissive permettent aux développeurs ou aux utilisateurs qui ne font pas partie du programme Apple pour les développeurs de tester les extensions de noyau avant qu'elles ne soient signées.

Une fois l'AuxKC créée, sa mesure est envoyée au Secure Enclave pour être signée et incluse dans une structure de données Image4 qui pourra être évaluée par iBoot au démarrage. Dans la cadre de la création de l'AuxKC, un reçu d'extension de noyau est également généré. Il contient la liste des extensions de noyau qui ont effectivement été incluses dans l'AuxKC, car l'ensemble pourrait être un sous-ensemble de l'UAKL si des extensions de noyau interdites étaient détectées. Un hachage SHA384 de la structure de données Image4 de l'AuxKC et un reçu d'extension de noyau sont inclus dans le fichier LocalPolicy. Le hachage Image4 de l'AuxKC est utilisé pour qu'iBoot puisse procéder à une vérification supplémentaire au démarrage afin de contribuer à empêcher le démarrage d'un ancien fichier Image4 de l'AuxKC signé par le Secure Enclave au moyen d'un fichier LocalPolicy plus récent. Le reçu de l'extension de noyau est utilisé par les sous-systèmes, comme Apple Pay, pour déterminer si des extensions de noyau susceptibles d'interférer avec la fiabilité de macOS sont actuellement chargées. Si tel est le cas, les fonctionnalités d'Apple Pay pourraient être désactivées.

Alternatives aux extensions de noyau (macOS 10.15 ou version ultérieure)

macOS 10.15 permet aux développeurs d'étendre les capacités de macOS en installant et en gérant des extensions système qui s'exécutent dans l'espace utilisateur plutôt qu'au niveau du noyau. En s'exécutant dans l'espace utilisateur, les extensions système augmentent la stabilité et la sécurité de macOS. Bien que les extensions de noyau aient pleinement accès à l'intégralité du système d'exploitation, les extensions exécutées dans l'espace utilisateur reçoivent uniquement les privilèges nécessaires à la réalisation de leur fonction indiquée.

Les développeurs peuvent utiliser des cadres d'application comme DriverKit, EndpointSecurity et NetworkExtension pour écrire des pilotes USB et d'interface humaine, des outils pour la sécurité des terminaux (comme la prévention des pertes de données ou d'autres agents de terminaux) ainsi que des outils VPN et réseau, le tout sans devoir écrire d'extensions de noyau. Des agents de sécurité tiers ne devraient être utilisés que s'ils tirent parti de ces API ou s'ils sont dotés d'une solide feuille de route pour passer à ces interfaces et délaisser les extensions du noyau.

Chargement des extensions de noyau approuvées par l'utilisateur

Pour une sécurité accrue, l'autorisation de l'utilisateur est exigée pour le chargement d'extensions de noyau installées en même temps que macOS 10.13 ou après la mise à niveau. On appelle ce processus le *chargement d'extensions de noyau approuvées par l'utilisateur*. L'autorisation de l'administrateur est requise pour approuver une extension du noyau. Les extensions de noyau ne nécessitent pas d'autorisation si elles :

- ont été installées sur un Mac sous macOS 10.12 ou une version antérieure;
- remplacent des extensions déjà approuvées;
- sont autorisées à s'exécuter sans l'approbation de l'utilisateur à l'aide de l'outil de ligne de commande `spctl` accessible à partir de recoveryOS;
- sont autorisées à s'exécuter à l'aide de la solution de gestion des appareils mobiles (GAM).

  Sous macOS 10.13.2 et les versions ultérieures, les utilisateurs peuvent utiliser la GAM pour préciser une liste d'extensions de noyau pouvant être chargées sans autorisation. Cette option nécessite un Mac exécutant macOS 10.13.2 inscrit à une solution de GAM par l'entremise d'Apple School Manager ou d'Apple Business Manager, ou manuellement par l'utilisateur.

Sécurité des mémoires mortes d'option sous macOS

Remarque : Les mémoires mortes d'option ne sont pas actuellement prises en charge sur les Mac avec puce Apple.

Sécurité des mémoires mortes d'option sur les Mac avec puce T2 Security d'Apple

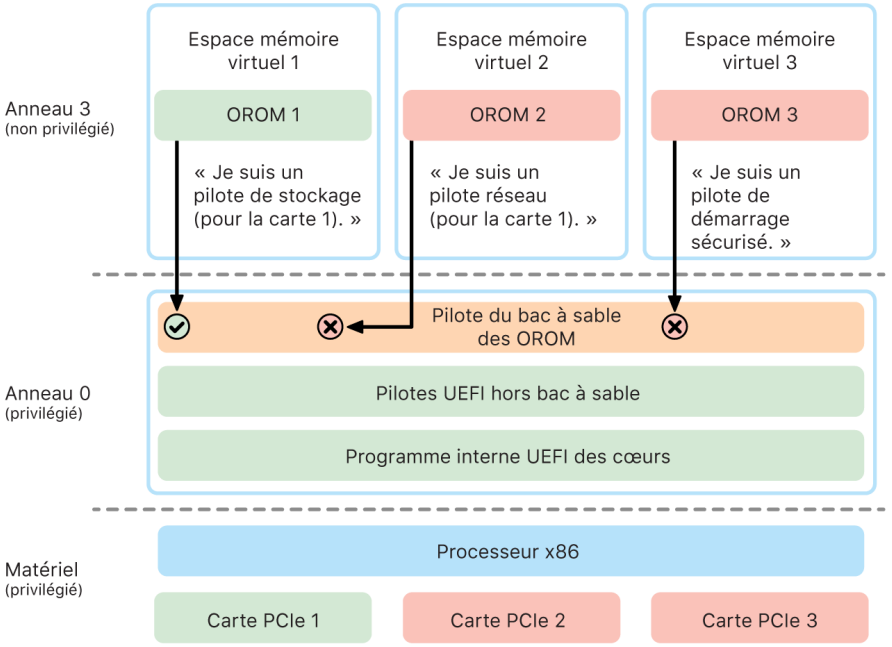
Les appareils Thunderbolt et PCIe peuvent être équipés d'une « mémoire morte d'option » (OROM) connectée par câble à l'appareil. (Il ne s'agit habituellement pas d'une véritable mémoire morte, mais plutôt d'une puce réinscriptible sur laquelle est stocké le programme interne.) Sur les appareils UEFI, ce programme interne est généralement un pilote UEFI qui est lu par le programme interne UEFI, puis exécuté. Le code exécuté est censé initialiser et configurer le matériel à partir duquel il est récupéré afin que ce matériel puisse être utilisable par le reste du programme interne. Cette fonctionnalité est requise pour que le matériel tiers spécialisé puisse se charger et fonctionner au début du démarrage, par exemple pour démarrer à partir des matrices de disques RAID externes.

Cependant, puisque les OROM sont généralement réinscriptibles, si un assaillant écrase l'OROM d'un périphérique légitime, son code s'exécutera tôt au cours du processus de démarrage et pourrait modifier l'environnement d'exécution et violer l'intégrité de logiciels chargés par la suite. De même, si l'assaillant introduit son propre dispositif malveillant dans le système, il pourra également exécuter un code malveillant.

Sous macOS 10.12.3, le comportement des ordinateurs Mac vendus après 2011 a été modifié pour ne pas exécuter les OROM par défaut au moment du démarrage du Mac, à moins que l'utilisateur appuie sur une certaine combinaison de touches. Cette combinaison de touches assurait une protection contre les OROM malveillantes introduites involontairement dans la séquence de démarrage de macOS. Le comportement par défaut de l'utilitaire de mot de passe de programme interne a également été modifié pour que les OROM ne puissent pas s'exécuter lorsque l'utilisateur réglait un mot de passe de programme interne, même si la combinaison de touches était entrée. Cette procédure empêchait un assaillant physiquement présent d'introduire une OROM malveillante. Pour les utilisateurs qui doivent quand même exécuter des OROM lorsque la protection par mot de passe de programme interne est activée, les réglages par défaut peuvent être modifiés à l'aide de l'outil de ligne de commande `firmwarepasswd` sous macOS.

Sécurité des OROM par mise en bac à sable

Sous macOS 10.15, le programme interne UEFI a été mis à jour et comporte maintenant un mécanisme de mise en bac à sable et de retrait des privilèges des OROM. Le programme interne UEFI, qui exécute typiquement tout le code, y compris les OROM, au niveau de privilège maximal (« anneau 0 ») du processeur central, dispose d'un seul espace mémoire virtuel partagé pour l'ensemble du code et des données. L'anneau 0 est le niveau de privilège auquel le noyau macOS s'exécute, tandis l'anneau 3 est le niveau de privilège inférieur auquel l'app s'exécute. Le bac à sable des OROM retire les privilèges des OROM en ayant recours, comme le fait le noyau, à la séparation de mémoire virtuelle, puis en exécutant les OROM dans l'anneau 3.



Mise en bac à sable des mémoires mortes d'option (OROM).

Le bac à sable restreint encore davantage les deux interfaces que les OROM peuvent appeler (tout comme le filtrage des appels système dans les noyaux) et le type d'appareil comme lequel une OROM peut s'enregistrer (similaire à l'approbation des apps). L'avantage de cette conception est que les OROM malveillantes ne peuvent plus écrire directement sur la mémoire de l'anneau 0. Elles sont plutôt limitées à une interface de bac à sable très étroite et bien définie. Cette interface limitée réduit considérablement la surface d'attaque et force les assaillants à s'échapper du bac à sable avant d'élever leurs privilèges.

Sécurité du programme interne UEFI des Mac avec processeur Intel

Aperçu

Depuis 2006, les ordinateurs Mac dotés d'un processeur Intel utilisent un programme interne Intel basé sur la première ou la deuxième version de la trousse de développement (EDK) de l'interface micrologicielle extensible (EFI). Le code EDK2 se conforme à la spécification de l'interface micrologicielle extensible unifiée (UEFI). Dans la présente section, le programme interne Intel est appelé *programme interne UEFI*. Le programme interne UEFI était le premier code exécuté sur la puce Intel.

Pour un Mac avec processeur Intel sans puce T2 Security d'Apple, la puce dans laquelle le programme interne est stocké constitue la base sécurisée du programme interne UEFI. Les mises à jour du programme interne UEFI sont signées numériquement par Apple et vérifiées par le programme interne avant la mise à jour du stockage. Pour contribuer à empêcher les attaques par retour en arrière, la version des mises à jour doit toujours être ultérieure à la version courante. Cependant, un assaillant ayant physiquement accès au Mac pourrait potentiellement utiliser du matériel pour accéder à la puce de stockage du programme interne et la mettre à jour afin d'insérer du contenu malveillant. De même, si des failles sont décelées tôt au cours du processus de démarrage du programme interne UEFI (avant la restriction en écriture de la puce de stockage), une infection persistante du programme interne UEFI pourrait avoir lieu. Il s'agit d'une limite de l'architecture matérielle courante dans la plupart des PC Intel et dans tous les ordinateurs Mac avec processeur Intel qui ne sont pas dotés de la puce T2.

Pour empêcher les attaques physiques qui sabotent le programme interne UEFI, l'architecture des ordinateurs Mac a été repensée de façon à enraciner la confiance envers le programme interne UEFI dans la puce T2. Sur ces ordinateurs Mac, c'est le programme interne T2 qui fait office de base sécurisée pour le programme interne UEFI, comme décrit dans la section Processus de démarrage d'un Mac avec processeur Intel.

Sous-composant du moteur de gestion Intel (ME)

Le programme interne du *moteur de gestion Intel (ME, Management Engine)* est un sous-composant stocké dans le programme interne UEFI. Le ME, un processeur et sous-système séparé dans les puces Intel, est utilisé principalement aux fins de la protection du droit d'auteur des contenus audio et vidéo sur un Mac doté uniquement de composants graphiques Intel. Afin de réduire la surface d'attaque de ce sous-composant, les Mac avec processeur Intel exécutent un programme interne ME personnalisé dont la plupart des composants ont été supprimés. Parce que le programme interne ME du Mac qui en résulte est moins volumineux que la version minimale par défaut proposée par Intel, de nombreux composants ayant déjà fait l'objet d'attaques par des chercheurs en sécurité informatique dans le secteur public n'existent plus.

Mode de gestion système (SMM)

Les processeurs Intel ont un mode d'exécution spécial qui est distinct du fonctionnement normal. Appelé *mode de gestion système (System Management Mode, SMM)*, il a été introduit à l'origine pour traiter les opérations dépendantes du temps telles que la gestion de la consommation. Or, pour effectuer ces opérations, les ordinateurs Mac ont toujours utilisé un microcontrôleur discret appelé *contrôleur de gestion du système (SMC, System Management Controller)*. Ce microcontrôleur n'est plus indépendant et est désormais intégré à la puce T2.

Sécurité du système sous watchOS

L'Apple Watch utilise en grande partie les mêmes fonctionnalités de sécurité matérielles pour sa plateforme qu'iOS et iPadOs. Par exemple, elle :

- exécute le démarrage sécurisé et les mises à jour logicielles sécurisées;
- maintient l'intégrité du système d'exploitation;
- contribue à la protection des données, autant sur l'appareil que lors des communications avec un iPhone jumelé ou l'Internet.

Les technologies prises en charge comprennent, outre celles énumérées dans la section Sécurité du système (par exemple KIP, SKP et SCIP), la protection des données, le trousseau et les technologies réseau.

Mise à jour du logiciel système

L'Apple Watch peut être configurée pour une mise à jour du logiciel système qui aura lieu la nuit même. Pour en savoir plus sur le stockage et l'utilisation du code de l'Apple Watch pendant la mise à jour, consultez la section Conteneurs de clés pour la protection des données.

Détection du poignet

Si la détection du poignet est activée, l'appareil est automatiquement verrouillé peu de temps après son retrait du poignet de l'utilisateur. Si la détection du poignet est désactivée, le centre de contrôle offre l'option de verrouiller l'Apple Watch. Quand l'Apple Watch est verrouillée, Apple Pay peut être utilisé uniquement après la saisie de son code. La détection du poignet peut être désactivée à l'aide de l'app Watch sur l'iPhone. Ce réglage peut également être appliqué à l'aide d'une solution de gestion des appareils mobiles (GAM).

Verrouillage d'activation

Lorsque la fonction Localiser est activée sur un iPhone, l'Apple Watch jumelée peut utiliser le verrouillage d'activation. Le verrouillage d'activation complique l'usage ou la revente d'une Apple Watch en cas de perte ou de vol. Il oblige l'utilisateur à saisir son identifiant Apple et son mot de passe pour déjumeler, effacer ou réactiver l'Apple Watch.

Jumelage sécurisé avec l'iPhone

L'Apple Watch peut être jumelée seulement avec un iPhone à la fois. Lorsque l'Apple Watch n'est pas jumelée, l'iPhone transmet des instructions pour effacer l'ensemble du contenu et des données de la montre.

Le jumelage de l'Apple Watch à l'iPhone est sécurisé grâce à un processus hors bande pour l'échange des clés publiques, puis à l'aide d'un secret partagé reposant sur une liaison Bluetooth faible énergie (BLE, Bluetooth Low Energy). L'Apple Watch affiche un motif animé, capté par la caméra de l'iPhone. Ce motif comporte un secret codé utilisé pour le jumelage hors bande BLE 4.1. La saisie de code d'accès BLE standard est employée comme méthode de jumelage de secours, si nécessaire.

Une fois la session BLE établie et chiffrée au moyen du protocole le plus sécurisé des spécifications principales de Bluetooth, l'iPhone et l'Apple Watch s'échangent des clés au moyen :

- soit d'un processus adapté à partir du service d'identité d'Apple (IDS), comme décrit dans l'aperçu de la sécurité d'iMessage;
- soit d'un échange de clés par l'entremise du protocole IKEv2/IPsec. L'échange de clés initial est authentifié soit au moyen de la clé de session Bluetooth (en cas de jumelage), soit au moyen de clés IDS (en cas de mise à jour du système d'exploitation). Chaque appareil génère une paire de clés publique et privée Ed25519 256 bits. Les clés publiques sont échangées au cours de l'échange de clés initial.

Remarque : Le mécanisme employé pour l'échange et le chiffrement des clés, selon la version des systèmes d'exploitation de l'iPhone et de l'Apple Watch. Les iPhone fonctionnant sous iOS 13 ou une version ultérieure qui sont jumelés à une Apple Watch fonctionnant sous watchOS 6 ou une version ultérieure utilisent uniquement le protocole IKEv2/IPsec pour échanger et chiffrer les clés.

Après l'échange des clés :

- La clé de session Bluetooth est abandonnée et toutes les communications entre l'iPhone et l'Apple Watch sont chiffrées par une des méthodes susmentionnées, les liaisons chiffrées Bluetooth, Wi-Fi et cellulaire fournissant une couche de chiffrement secondaire.
- (IKEv2/IPsec uniquement) Les clés sont stockées dans le trousseau du système et utilisées pour authentifier les futures sessions IKEv2/IPsec entre les appareils. Les futures communications entre ces appareils seront chiffrées, et leur intégrité sera protégée par ChaCha20-Poly1305 (des clés 256 bits).

L'adresse BLE de l'appareil est remplacée toutes les 15 minutes pour réduire le risque qu'un appareil soit suivi localement si quelqu'un diffuse un identifiant permanent.

Pour les apps requérant des données de diffusion en continu, le chiffrement est assuré à l'aide des méthodes décrites dans la section Sécurité de FaceTime, en faisant appel à l'IDS fourni par l'iPhone jumelé ou à une connexion Internet directe.

L'Apple Watch implémente du stockage chiffré matériellement et une protection basée sur des classes pour les fichiers et les éléments du trousseau. Des conteneurs de clés dont l'accès est contrôlé sont également utilisés pour les éléments de trousseau. Les clés employées pour la communication entre l'Apple Watch et l'iPhone sont aussi sécurisées à l'aide d'une protection basée sur des classes. Pour en savoir plus, consultez la section Conteneurs de clés pour la protection des données.

Déverrouillage automatique et Apple Watch

Pour une meilleure commodité lors de l'utilisation de plusieurs appareils Apple, certains d'entre eux peuvent automatiquement déverrouiller les autres dans certaines situations. Le déverrouillage automatique est possible dans trois situations :

- Un iPhone peut déverrouiller une Apple Watch.
- Une Apple Watch peut déverrouiller un Mac.
- Une Apple Watch peut déverrouiller un iPhone après la détection d'un utilisateur dont la bouche et le nez sont couverts.

Ces trois usages s'appuient sur la même base : un protocole Station-to-Station (STS) à authentification mutuelle, avec des clés à long échangées au moment de l'activation de la fonctionnalité et des clés de session éphémères uniques pour chaque demande. Peu importe le canal de communication sous-jacent, le tunnel STS est négocié directement entre les Secure Enclave des deux appareils, et le matériel de chiffrement est conservé à l'intérieur de ce domaine sécurisé (à l'exception des ordinateurs Mac sans Secure Enclave, pour lesquels le tunnel STS prend fin dans le noyau).

Déverrouillage

Une séquence de déverrouillage complète comporte deux phases. D'abord, l'appareil à déverrouiller (la « cible ») génère un secret de déverrouillage cryptographique qu'il envoie à l'appareil procédant au déverrouillage (l'« initiateur »). Ensuite, l'initiateur effectue le déverrouillage au moyen du secret généré.

Pour armer le déverrouillage, les appareils se connectent l'un à l'autre par une connexion BLE. Un secret de déverrouillage de 32 octets aléatoirement généré par l'appareil cible est envoyé à l'initiateur via le tunnel STS. Lors du prochain déverrouillage par biométrie ou par code, l'appareil cible enveloppe sa clé dérivée du code (PDK) avec le secret de déverrouillage et élimine celui-ci de sa mémoire.

Pour effectuer le déverrouillage, les appareils établissent une nouvelle connexion BLE avant d'utiliser le Wi-Fi pair à pair pour estimer en toute sécurité la distance qui les sépare. S'ils se trouvent à l'intérieur de la portée établie et que les règlements de sécurité requis sont respectés, l'initiateur envoie son secret de déverrouillage à la cible via le tunnel STS. La cible génère ensuite un nouveau secret de déverrouillage de 32 octets qu'elle renvoie à l'initiateur. Si le secret de déverrouillage en vigueur envoyé par l'initiateur arrive à déchiffrer l'enregistrement de déverrouillage, l'appareil cible est déverrouillé et la PDK est enveloppée de nouveau avec un autre secret de déverrouillage. Finalement, le nouveau secret de déverrouillage et la PDK sont éliminés de la mémoire de la cible.

Règlements de sécurité du déverrouillage automatique de l'Apple Watch

Pour plus de commodité, un iPhone peut déverrouiller l'Apple Watch directement après son démarrage initial sans que l'utilisateur ait à saisir d'abord le code sur l'Apple Watch. Pour y arriver, le secret de déverrouillage aléatoire (généré lors de la toute première séquence de déverrouillage après l'activation de la fonctionnalité) est utilisé pour créer une autorité de séquestre à long terme stockée dans le conteneur de clés de l'Apple Watch. Le secret de l'enregistrement sous séquestre est stocké dans le trousseau de l'iPhone et utilisé pour amorcer une nouvelle session après chaque redémarrage de l'Apple Watch.

Règlements de sécurité du déverrouillage automatique de l'iPhone

Des règlements de sécurité supplémentaires s'appliquent au déverrouillage automatique de l'iPhone avec l'Apple Watch. L'Apple Watch ne peut pas remplacer Face ID sur l'iPhone pour d'autres opérations comme Apple Pay ou les autorisations d'app. Lorsque l'Apple Watch déverrouille un iPhone jumelé, la montre affiche une notification et émet une vibration associée. Si l'utilisateur touche le bouton « Verrouiller l'iPhone » de la notification, la montre envoie à l'iPhone une commande de verrouillage via BLE. Lorsque l'iPhone reçoit la commande de verrouillage, il se verrouille et désactive Face ID ainsi que le déverrouillage avec l'Apple Watch. Le prochain déverrouillage de l'iPhone doit être effectué au moyen de son code.

Pour déverrouiller un iPhone jumelé à partir de l'Apple Watch (lorsque la fonctionnalité est activée), il faut respecter les critères suivants :

- L'iPhone doit avoir été déverrouillé au moyen d'une autre méthode au moins une fois après que l'Apple Watch associée a été placée sur le poignet et déverrouillée.
- Les capteurs doivent pouvoir détecter que la bouche et le nez de l'utilisateur sont couverts.
- La distance mesurée doit être de 2 à 3 mètres ou moins.
- Le mode Sommeil ne doit pas être activé sur l'Apple Watch.
- L'Apple Watch ou l'iPhone doit avoir été déverrouillé récemment, ou l'Apple Watch doit avoir détecté un mouvement indiquant que la personne qui la porte est active (c'est-à-dire qu'elle ne dort pas).
- L'iPhone doit avoir été déverrouillé moins de six heures et demie auparavant.
- L'iPhone doit être dans un état qui permet à Face ID de déverrouiller l'appareil. (Pour en savoir plus, consultez la section Touch ID, Face ID, les codes et les mots de passe.)

Approbation sous macOS avec l'Apple Watch

Lorsque le déverrouillage automatique est activé, l'Apple Watch peut être utilisée à la place de Touch ID ou avec Touch ID pour approuver les invites d'autorisation et d'authentification :

- des apps macOS et Apple qui demandent une autorisation;
- des apps tierces qui demandent une authentification;
- des mots de passe Safari enregistrés;
- des notes sécurisées.

Utilisation sécurisée du Wi-Fi, des données cellulaires, d'iCloud et de Gmail

Si l'Apple Watch est hors de portée du signal Bluetooth, une connexion Wi-Fi ou cellulaire peut être utilisée à la place. L'Apple Watch se connecte automatiquement aux réseaux Wi-Fi auxquels l'iPhone jumelé s'est déjà connecté et dont les informations d'identification ont été synchronisées avec l'Apple Watch alors que les deux appareils étaient à portée l'un de l'autre. Dans la section Wi-Fi de l'app Réglages sur l'Apple Watch, il est possible de configurer la connexion automatique au cas par cas selon les réseaux et de se connecter manuellement aux réseaux Wi-Fi auxquels aucun des deux appareils ne s'est déjà connecté.

Si l'Apple Watch est hors de portée de l'iPhone, elle se connecte directement aux serveurs iCloud et Gmail pour récupérer les courriels plutôt que de synchroniser par Internet les données Mail avec l'iPhone jumelé. Pour les comptes Gmail, l'utilisateur doit s'authentifier auprès de Google dans la section Mail de l'app Watch sur l'iPhone. Le jeton OAuth reçu de Google est transmis à l'Apple Watch dans un format chiffré à l'aide du service d'identité d'Apple (IDS) afin qu'il puisse être utilisé pour récupérer les courriels. Ce jeton OAuth n'est jamais utilisé pour se connecter au serveur Gmail depuis l'iPhone jumelé.

Génération de nombres aléatoires

Les générateurs de nombres pseudo-aléatoires cryptographiques (CPRNG) sont un élément important d'un logiciel sécurisé. C'est pourquoi Apple offre un CPRNG logiciel de confiance, qui est exécuté dans les noyaux iOS, iPadOS, macOS, tvOS et watchOS. C'est ce CPRNG qui accumule l'entropie brute du système et distribue des nombres aléatoires sécurisés aux consommateurs dans le noyau et dans l'espace utilisateur.

Sources d'entropie

Le CPRNG du noyau est alimenté par plusieurs sources d'entropie pendant le démarrage et toute la durée de vie de l'appareil. Ces sources comprennent (selon la disponibilité) :

- le générateur de nombres aléatoires (TRNG) matériel du Secure Enclave;
- la gigue de synchronisation relevée pendant le démarrage;
- l'entropie obtenue des interruptions matérielles;
- un fichier source utilisé pour conserver l'entropie entre les démarrages;
- les instructions aléatoires d'Intel, par exemple RDSEED et RDRAND (uniquement sur les Mac avec processeur Intel).

CPRNG du noyau

Le CPRNG du noyau est une conception dérivée de Fortuna, qui vise un niveau de sécurité 256 bits. Il fournit des nombres aléatoires de haute qualité aux consommateurs de l'espace utilisateur par les API suivantes :

- l'appel système `getentropy`(2);
- le fichier spécial (/dev/random).

Le CPRNG du noyau accepte l'entropie fournie par l'utilisateur via l'écriture sur le fichier spécial.

Appareil de recherche en sécurité d'Apple

L'appareil de recherche en sécurité informatique d'Apple est un iPhone doté d'un « fusible » spécial qui permet aux chercheurs en sécurité informatique de mener des travaux sur iOS sans avoir à contourner ou à désactiver les fonctionnalités de sécurité de la plateforme. Grâce à cet appareil, les chercheurs sont en mesure de charger des contenus non vérifiés par Apple qui pourront s'exécuter avec un niveau d'autorisation équivalent à celui de la plateforme, et donc de travailler sur une plateforme plus proche de celle des appareils de production.

Pour contribuer à éviter que les appareils d'utilisateur soient touchés par le règlement d'exécution des appareils de recherche, les modifications du règlement sont implémentées dans une variante d'iBoot et la collection du noyau de démarrage. Ces modifications sont vouées à l'échec sur les appareils d'utilisateur. Si elles sont exécutées sur un appareil qui n'est pas destiné à la recherche, l'iBoot de recherche cherche un autre état de fusion et déclenche alors une boucle d'erreurs graves (ou de panique).

Le sous-système cryptex permet aux chercheurs de charger un cache de confiance personnalisé et une image disque qui contient du contenu qui s'y rattache. De nombreuses mesures détaillées de défense ont été implémentées pour empêcher ce sous-système d'autoriser toute exécution sur tout appareil d'utilisateur :

- `launchd` ne chargera pas la liste de propriétés launchd de `cryptexd` s'il n'est pas en mesure de détecter le fusible de recherche.
- `cryptexd` abandonne l'opération s'il ne détecte pas le fusible de recherche.
- Le droit qui octroie à `cryptexd` la capacité de monter une image disque est honoré uniquement par le cache du noyau de recherche. Le chemin du code approprié n'est pas compilé dans le cache du noyau standard.
- Le serveur de signature refuse de personnaliser l'image disque cryptex pour tout appareil qui ne figure pas dans une liste d'autorisation explicite.

Pour préserver les données personnelles des chercheurs en sécurité informatique, seules les mesures (des hachages, par exemple) des exécutables et les identifiants de l'appareil de recherche sont envoyés à Apple pendant la personnalisation. Apple ne reçoit pas le contenu du cryptex qui est chargé sur l'appareil.

Pour éviter qu'une personne malveillante tente de faire passer un appareil de recherche pour un appareil d'utilisateur afin d'amener une cible à l'utiliser au quotidien, l'appareil de recherche en sécurité présente les différences suivantes :

- L'appareil de recherche en sécurité ne démarre que lorsqu'il est branché sur une source d'alimentation, ce qui peut être au moyen d'un câble Lightning ou d'un chargeur Qi compatible. Si l'appareil n'est pas branché à une source d'alimentation lorsqu'il démarre, il entre en mode de récupération. Si l'utilisateur branche l'appareil et le met en marche, celui-ci démarre normalement. Dès que le noyau XNU démarre, l'appareil n'a pas besoin de rester branché sur une source d'alimentation pour fonctionner.
- La mention *Security Research Device* (appareil de recherche en sécurité) s'affiche sous le logo Apple lors du démarrage d'iBoot.
- Le noyau XNU démarre en mode détaillé.
- Un message est gravé en anglais sur le côté de l'appareil : « Property of Apple. Confidential and Proprietary. Call +1 877 595 1125. »

Les mesures supplémentaires suivantes sont implémentées dans les logiciels qui apparaissent après le démarrage :

- La mention *Security Research Device* s'affiche lors de la configuration de l'appareil.
- La mention *Security Research Device* s'affiche sur l'écran verrouillé et dans l'app Réglages.

L'appareil de recherche en sécurité accorde aux chercheurs les possibilités suivantes qui ne sont pas offertes sur un appareil d'utilisateur :

- charger sur l’appareil du code exécutable non signé par Apple avec des droits arbitraires au même niveau d’autorisation que les composants du système d’exploitation d’Apple;
- démarrer des services au démarrage de l’appareil;
- faire persister des contenus d’un redémarrage à l’autre.

Chiffrement et protection des données

Aperçu du chiffrement et de la protection des données

La chaîne de démarrage sécurisée, la sécurité du système et les fonctionnalités de sécurité des apps contribuent à faire en sorte que seuls des apps et du code vérifiés s'exécutent sur l'appareil. En outre, des fonctions de chiffrement additionnelles assurent la protection des données même lorsque certaines parties de l'infrastructure de sécurité ont été compromises (par exemple si l'appareil a été perdu ou s'il exécute du code non vérifié). Et parce que les renseignements personnels et ceux de l'entreprise sont protégés et que les données d'un appareil perdu ou volé peuvent être entièrement effacées à distance en un instant, tout cela profite aux utilisateurs comme aux administrateurs des TI.

Les appareils iOS et iPadOS utilisent une méthode de chiffrement des fichiers appelée *protection des données*, tandis que les Mac à processeur Intel sont protégés par la technologie de chiffrement de disque *FileVault*. Les Mac dotés d'une puce Apple utilisent quant à eux un modèle hybride compatible avec la protection des données, à deux nuances près : le niveau de protection le plus bas (classe D) n'est pas pris en charge, d'une part, et le niveau par défaut (classe C) utilise une clé de volume et se comporte exactement comme FileVault sur un Mac à processeur Intel, d'autre part. Dans tous les cas, les hiérarchies de gestion des clés sont ancrées dans la puce du Secure Enclave prévue à cette fin, et un moteur AES dédié permet le chiffrement pleine vitesse tout en veillant à ce que les clés de chiffrement longue durée ne soient jamais transmises au noyau du système d'exploitation ou au processeur central, où elles pourraient être compromises. (Un Mac à processeur Intel équipé d'une puce T1 ou dépourvu de Secure Enclave n'a pas de puce dédiée pour protéger ses clés de chiffrement FileVault.)

Outre le recours à la protection des données et à FileVault pour contribuer à empêcher tout accès non autorisé à l'information, Apple utilise les *noyaux de système d'exploitation* pour renforcer la protection et la sécurité. Les noyaux utilisent des contrôles d'accès pour mettre les apps en bac à sable (ce qui restreint les données auxquelles ces apps ont accès) ainsi qu'un mécanisme appelé *Data Vault* (qui, au lieu de limiter les appels pouvant être passés par une app, restreint l'accès aux données d'une app par toutes les autres apps qui en font la demande).

Codes et mots de passe

Codes sur les appareils prenant en charge la protection des données

En configurant un code ou un mot de passe pour son appareil, l'utilisateur active automatiquement la protection des données. iOS et iPadOS prennent en charge les codes à six chiffres, les codes à quatre chiffres et les codes alphanumériques de longueur arbitraire. En plus de déverrouiller l'appareil, le code ou le mot de passe fournit l'entropie pour certaines clés de chiffrement. Cela veut dire que, sans le code de sécurité, un assaillant en possession d'un appareil ne peut accéder aux données appartenant à certaines classes de protection.

Le code ou le mot de passe étant emmêlé avec l'UID de l'appareil, des attaques en force sont nécessaires pour tenter d'accéder à l'appareil. Un grand nombre d'itérations est utilisé pour ralentir chaque tentative. Ce nombre d'itérations est étalonné de sorte qu'une tentative prenne environ 80 millisecondes. En fait, il faudrait plus de cinq ans et demi pour essayer toutes les combinaisons d'un code alphanumérique à six caractères composé de lettres minuscules et de chiffres.

Plus le code de l'utilisateur est complexe, meilleure est la clé de chiffrement. De plus, en utilisant Touch ID ou Face ID, l'utilisateur peut établir un code beaucoup plus robuste que ce qui serait autrement pratique. Ce code augmente le degré réel d'entropie protégeant les clés de chiffrement utilisées pour la protection des données, sans nuire à l'expérience de l'utilisateur qui déverrouille son appareil maintes fois par jour.

Pour compliquer encore davantage les attaques en force, des délais de plus en plus longs sont prévus après la saisie d'un code non valide sur l'écran verrouillé.

Délais entre les tentatives de déverrouillage par code

Tentatives	Délai imposé
1 à 4	Aucune
5	1 minute
6	5 minutes
7 à 8	15 minutes
9	1 heure

Si l'option « Effacer les données » est activée (dans Réglages > Touch ID et code), après 10 tentatives infructueuses de déverrouillage par code, l'intégralité du contenu et des réglages est supprimée du stockage. Les tentatives consécutives du même mauvais code ne comptent pas dans la limite. Ce réglage peut également être imposé par une politique d'entreprise via une solution de gestion des appareils mobiles (GAM) qui prend en charge cette fonctionnalité et via Microsoft Exchange ActiveSync, de même qu'être fixé à un seuil inférieur.

Sur les appareils qui en sont dotés, les délais sont imposés par le Secure Enclave. Le redémarrage de l'appareil n'annule pas le délai imposé, mais a pour effet de réinitialiser la minuterie.

Définition de codes plus longs

Si un long mot de passe qui ne contient que des chiffres est entré, un pavé numérique s'affiche sur l'écran verrouillé à la place du clavier complet. Un code numérique de longueur importante peut être plus facile à saisir qu'un code alphanumérique court, tout en fournissant un niveau de sécurité identique.

Les utilisateurs peuvent indiquer un code alphanumérique plus long en sélectionnant « Code alphanumérique personnalisé » comme Options de code dans Réglages > Touch ID et code ou Face ID et code.

Délais entre les tentatives de déverrouillage par mot de passe sous macOS

Pour contribuer à prévenir les attaques en force, un maximum de dix tentatives de déverrouillage par mot de passe est autorisé dans la fenêtre de connexion ou en mode disque cible au démarrage du Mac, et des délais de plus en plus longs sont imposés après un certain nombre de tentatives. Ces délais sont imposés par le Secure Enclave. Le redémarrage du Mac n'annule pas le délai imposé, mais a pour effet de réinitialiser la minuterie.

Pour contribuer à empêcher les logiciels malveillants de causer des pertes de données permanentes en tentant d'attaquer le mot de passe de l'utilisateur, ces limites ne sont plus imposées une fois que l'utilisateur a réussi à se connecter au Mac, mais elles le sont de nouveau après un redémarrage. Si les dix tentatives sont épuisées, dix tentatives supplémentaires sont possibles après un démarrage sous recoveryOS. Si ces tentatives sont aussi épuisées, dix sont disponibles pour chaque mécanisme de récupération FileVault (récupération iCloud, clé de secours FileVault et clé institutionnelle), pour un maximum de trente tentatives supplémentaires. Après l'épuisement de ces tentatives supplémentaires, le Secure Enclave ne traite plus aucune demande de déchiffrement du volume ou de vérification du mot de passe, et les données sur le disque ne sont plus récupérables.

Pour protéger les données en entreprise, les équipes des TI doivent définir une politique claire pour la configuration de FileVault et l'imposer par l'intermédiaire d'une solution de GAM. Les organisations disposent de plusieurs options pour la gestion des volumes chiffrés, comme les clés de secours institutionnelles, les clés de secours personnelles (qui peuvent être enregistrées dans la solution de GAM pour l'autorité de séquestre), ou une combinaison des deux. La rotation de clés peut elle aussi faire l'objet d'une politique de GAM.

Délais entre les tentatives de déverrouillage par mot de passe sur un Mac doté d'une puce Apple ou de la puce T2

Tentatives	Délai imposé
5	1 minute

Tentatives	Délai imposé
6	5 minutes
7	15 minutes
8	15 minutes
9	1 heure
10	Désactivation

Sur un Mac doté de la puce T2 Security d'Apple, le mot de passe assure une fonction similaire, sauf que la clé générée est utilisée pour le chiffrement FileVault plutôt que la protection des données. macOS propose également d'autres options de récupération de mot de passe :

- récupération iCloud;
- récupération FileVault;
- clé institutionnelle FileVault.

Protection des données

Aperçu de la protection des données

Apple utilise une technologie appelée protection des données pour renforcer la sécurité des données enregistrées dans le stockage flash des appareils dotés d'un système sur une puce d'Apple, comme les iPhone, les iPad, les Apple Watch, les Apple TV et les Mac avec puce Apple. La protection des données permet à l'appareil de répondre à des événements courants comme les appels téléphoniques entrants, tout en assurant un niveau de chiffrement élevé des données utilisateur. Certaines apps système (comme Messages, Mail, Calendrier, Contacts et Photos) et les données de Santé utilisent la protection des données par défaut. Les apps tierces bénéficient automatiquement de cette protection.

Mise en œuvre

La protection des données est mise en œuvre en élaborant et en gérant une hiérarchie de clés, et repose sur les technologies de chiffrement matériel intégrées aux appareils Apple. Elle est contrôlée fichier par fichier en attribuant une classe à chacun d'eux; l'accessibilité est déterminée en fonction de l'état de déverrouillage des clés de classe. Le système de fichiers d'Apple (APFS) permet de subdiviser les clés par domaine (ce qui permet aux parties d'un fichier d'avoir différentes clés).

Chaque fois qu'un fichier est créé sur le volume de données, la protection des données génère une nouvelle clé de 256 bits (la clé « par fichier ») et la transmet au moteur AES matériel. Sur les appareils dotés d'un système sur une puce A14 ou M1, le chiffrement utilise l'algorithme AES-256 dans un mode d'opération de chiffrement par blocs appelé XTS, où la clé par fichier de 256 bits passe par une fonction de dérivation de clés (publication spéciale 800-108 du NIST) pour obtenir une valeur « tweak » de 256 bits et une clé de chiffrement de 256 bits. Le matériel de génération A9 à A13 ainsi que S5 et S6 utilise l'algorithme AES-128 en mode XTS, où la clé par fichier de 256 bits est répartie de manière à offrir une valeur « tweak » de 128 bits et une clé de chiffrement de 128 bits.

Sur un Mac avec puce Apple, la protection des données est réglée par défaut à la classe C (consultez la section Classes de protection des données), mais elle utilise une clé de volume au lieu d'une clé par domaine ou par fichier, recréant ainsi le modèle de sécurité de FileVault pour les données utilisateur. Les utilisateurs doivent malgré tout choisir d'utiliser FileVault pour bénéficier de la protection complète offerte par l'emmêlement de la hiérarchie des clés de chiffrement avec leur mot de passe. Les développeurs peuvent aussi choisir une classe de protection plus élevée qui utilise une clé par fichier ou par domaine.

Protection des données sur les appareils Apple

Sur les appareils Apple qui utilisent la protection des données, chaque fichier est protégé à l'aide d'une clé par fichier (ou par domaine) unique. La clé, enveloppée à l'aide de l'algorithme d'encapsulation de clé NIST AED, est enveloppée une autre fois par une des différentes clés de classe, en fonction du mode d'accès au fichier. La clé par fichier enveloppée est stockée dans les métadonnées du fichier.

Les appareils dotés du format APFS peuvent prendre en charge le clonage des fichiers (copies sans perte à l'aide de la technologie de copie à l'écriture). Si un fichier est cloné, chaque moitié du clone obtient une nouvelle clé pour accepter les écritures entrantes de façon à ce que les nouvelles données y soient inscrites avec une nouvelle clé. Au fil du temps, le fichier peut être composé de différents domaines (ou fragments), chacun associé à une clé différente. Cependant, tous les domaines qui forment un même fichier sont protégés par la même clé de classe.

Lorsqu'un fichier est ouvert, ses métadonnées sont déchiffrées à l'aide de la clé du système de fichiers, ce qui révèle la clé par fichier enveloppée ainsi que la classe qui la protège. La clé par fichier (ou par domaine) est débloquée avec la clé de classe, puis transmise au moteur AES matériel, qui déchiffre le fichier au moment de sa lecture à partir du stockage flash. Toute la gestion des clés par fichier enveloppées se fait dans le Secure Enclave; la clé de fichier n'est jamais directement exposée au processeur d'application. Au démarrage, le Secure Enclave négocie une clé éphémère avec le moteur AES. Quand le Secure Enclave débloque les clés d'un fichier, celles-ci sont enveloppées avec la clé éphémère, puis envoyées au processeur d'application.

Les métadonnées de tous les fichiers présents dans le système de fichiers du volume de données sont chiffrées avec une clé aléatoire, qui est créée lors de l'installation initiale du système d'exploitation ou lors de l'effacement de l'appareil par l'utilisateur. Cette clé est chiffrée et enveloppée par une clé d'encapsulation connue uniquement du Secure Enclave pour le stockage à long terme. La clé d'encapsulation change chaque fois qu'un utilisateur efface son appareil. Sur les systèmes sur une puce A9 et de génération ultérieure, le Secure Enclave compte sur une entropie renforcée par des systèmes antirejeu pour réaliser l'effacement et protéger, entre autres, sa clé d'encapsulation. Pour en savoir plus, consultez la section Stockage non volatil sécurisé.

Tout comme les clés par fichier ou par domaine, la clé de métadonnées du volume de données n'est jamais exposée directement au processeur d'application; le Secure Enclave en envoie plutôt une version éphémère, qui change à chaque démarrage. Lorsqu'elle est stockée, la clé chiffrée du système de fichiers est par ailleurs enveloppée par une « clé effaçable » stockée dans le stockage effaçable ou par une clé d'encapsulation de clé de support, protégée par le mécanisme antirejeu du Secure Enclave. Cette clé ne renforce pas la confidentialité des données. Elle est plutôt conçue pour être effacée rapidement sur demande (par l'utilisateur, à l'aide de l'option « Effacer contenu et réglages », ou par un utilisateur ou un administrateur qui exécute une commande d'effacement à distance via une solution de GAM, Microsoft Exchange ActiveSync ou iCloud). Effacer la clé de cette manière rend impossible le déchiffrement des fichiers.

Le contenu d'un fichier peut être chiffré avec des clés par fichier (ou par domaine), qui sont enveloppées avec une clé de classe et stockées dans les métadonnées du fichier, qui sont à leur tour chiffrées avec la clé du système de fichiers. La clé de classe est protégée par l'UID de l'appareil et, pour certaines classes, par le code de l'utilisateur. Cette hiérarchie offre à la fois souplesse et performance. Par exemple, pour changer la classe d'un fichier, il suffit d'envelopper de nouveau sa clé par fichier; la modification du code de sécurité n'enveloppe de nouveau que la clé de classe.

Classes de protection des données

Lorsqu'un nouveau fichier est créé sur des appareils prenant en charge la protection des données, une classe lui est attribuée par l'app dont il est issu. Chaque classe utilise des règles différentes pour déterminer quand les données sont accessibles. Les classes et règles de base sont décrites dans les sections qui suivent. Les ordinateurs Mac avec puce Apple ne prennent pas en charge la classe D (Aucune protection) et une limite de sécurité est établie autour des opérations de connexion et de déconnexion (et non pas de verrouillage et de déverrouillage, comme sur les iPhone, les iPad et les iPod touch).

Classe	**Type de protection**
Classe A : Protection complète	(NSFileProtectionComplete)
Classe B : Protection complète sauf si des données sont ouvertes	(NSFileProtectionCompleteUnlessOpen)
Classe C : Protection complète jusqu'à la première authentification de l'utilisateur *Remarque :* macOS utilise une clé de volume pour recréer les caractéristiques de la protection offerte par FileVault.	(NSFileProtectionCompleteUntilFirstUser Authentication)
Classe D : Aucune protection *Remarque :* Non pris en charge sous macOS.	(NSFileProtectionNone)

Protection complète

(NSFileProtectionComplete) : La clé de classe est protégée par une clé obtenue à partir du code ou du mot de passe de l'utilisateur, et de l'UID de l'appareil. Peu après que l'utilisateur a verrouillé l'appareil (10 secondes, quand le réglage Exiger le mot de passe est réglé sur « immédiatement »), la clé de classe déchiffrée est détruite, ce qui rend inaccessibles toutes les données de cette classe jusqu'à ce que l'utilisateur entre de nouveau son code ou déverrouille l'appareil (s'y connecte) avec Touch ID ou Face ID.

Sous macOS, peu après la déconnexion du dernier utilisateur, la clé de classe déchiffrée est détruite, rendant toutes les données de cette classe inaccessibles jusqu'à ce qu'un utilisateur entre de nouveau son code ou se connecte à l'appareil avec Touch ID.

Protection complète sauf si des données sont ouvertes

(NSFileProtectionCompleteUnlessOpen) : Cette classe permet l'écriture de fichiers lorsque l'appareil est verrouillé ou lorsque l'utilisateur s'est déconnecté. Le téléchargement en arrière-plan d'une pièce jointe à un courriel en est un bon exemple. La technologie utilisée est la cryptographie asymétrique à courbe elliptique (ECDH avec Curve25519). La clé par fichier habituelle est protégée par une clé obtenue au moyen d'un protocole d'échange Diffie-Hellman à une passe décrit dans la publication spéciale 800-56A du NIST.

La clé publique éphémère de l'échange est stockée avec la clé par fichier enveloppée. La méthode de dérivation de clé est la concaténation (solution approuvée 1), décrite dans la section 5.8.1 de la même publication. AlgorithmID est omis. PartyUInfo et PartyVInfo correspondent respectivement à la clé publique éphémère et à la clé publique statique. La fonction de hachage utilisée est SHA256. À la fermeture du fichier, la clé par fichier est effacée de la mémoire. Pour rouvrir le fichier, le secret partagé est recréé à l'aide de la clé privée de la classe « Protection complète sauf si des données sont ouvertes » et de la clé publique éphémère du fichier, lesquelles servent à débloquer la clé par fichier, qui peut alors déchiffrer le fichier.

Sous macOS, la partie privée de NSFileProtectionCompleteUnlessOpen est accessible aussi longtemps qu'un utilisateur est connecté ou authentifié sur le système.

Protection complète jusqu'à la première authentification de l'utilisateur

(NSFileProtectionCompleteUntilFirstUserAuthentication) : Cette classe fonctionne de la même façon que la « Protection complète », sauf que la clé de classe déchiffrée n'est pas effacée de la mémoire lorsque l'appareil est verrouillé ou lorsque l'utilisateur s'est déconnecté. Cette classe offre des propriétés semblables au chiffrement complet du disque sur les ordinateurs de bureau et protège les données des attaques comprenant un redémarrage. Elle est attribuée par défaut à toutes les données d'apps tierces non attribuées à une classe de protection des données.

Sous macOS, cette classe utilise une clé de volume qui est accessible tant que le volume est monté et qui fonctionne exactement comme FileVault.

Aucune protection

(NSFileProtectionNone) : Cette clé de classe n'est protégée que par l'UID et est entreposée dans le stockage effaçable. Puisque toutes les clés requises pour déchiffrer les fichiers dans cette classe sont entreposées sur l'appareil, le seul avantage que présente ce type de chiffrement est l'effacement à distance rapide. Les fichiers auxquels aucune classe de protection n'est attribuée sont quand même stockés sous forme chiffrée, comme toutes les données sur les appareils iOS et iPadOS.

Ceci n'est pas pris en charge sous macOS.

Remarque : Sous macOS, en ce qui concerne les volumes qui ne correspondent pas à un système d'exploitation démarré, toutes les classes de protection des données restent accessibles tant que le volume est monté. La classe de protection des données par défaut est *NSFileProtectionCompleteUntilFirstUserAuthentication*. La fonctionnalité de la clé par domaine est disponible pour Rosetta 2 et les apps natives.

Conteneurs de clés pour la protection des données

Les clés destinées aux classes de protection des données pour les fichiers et le trousseau sont recueillies et gérées dans des conteneurs de clés sous iOS, iPadOS, watchOS et tvOS. Ces systèmes d'exploitation utilisent les conteneurs de clés suivants : utilisateur, appareil, sauvegarde, séquestre et sauvegarde iCloud.

Conteneur de clés de l'utilisateur

Le conteneur de clés de l'utilisateur est l'endroit où sont stockées les clés de classe enveloppées utilisées lors du fonctionnement normal de l'appareil. Par exemple, lorsqu'un code est entré, la clé *NSFileProtectionComplete* est chargée à partir du conteneur de clés de l'utilisateur et développée. Il s'agit d'un fichier binaire de liste de propriétés (.plist) appartenant à la classe « Aucune protection ».

Pour les appareils dotés d'un système sur une puce de génération antérieure à A9, le contenu du fichier .plist est chiffré à l'aide d'une clé stockée dans le stockage effaçable. Afin d'assurer la sécurité à terme des conteneurs de clés, cette clé est effacée et régénérée chaque fois qu'un utilisateur modifie son code.

Pour les appareils dotés d'un système sur une puce A9 ou de génération ultérieure, le fichier .plist contient une clé qui indique que le conteneur de clés est stocké dans un casier protégé par le nonce antirejeu contrôlé par le Secure Enclave.

Le Secure Enclave gère le conteneur de clés de l'utilisateur et peut être interrogé sur l'état de verrouillage d'un appareil. Il signale que l'appareil est déverrouillé uniquement si toutes les clés de classe du conteneur de clés de l'utilisateur sont accessibles et qu'elles sont correctement débloquées.

Conteneur de clés de l'appareil

Le conteneur de clés de l'appareil sert à stocker les clés de classe enveloppées qui sont utilisées pour les opérations qui touchent des données propres à l'appareil. Les appareils iPadOS configurés pour une utilisation partagée doivent parfois accéder aux informations d'identification avant qu'un utilisateur ne soit connecté. Dès lors, un conteneur de clés qui n'est pas protégé par le code de l'utilisateur est nécessaire.

iOS et iPadOS ne prennent pas en charge la séparation cryptographique du contenu du système de fichiers propre à l'utilisateur, ce qui signifie que le système utilise les clés de classe tirées du conteneur de clés de l'appareil pour envelopper les clés par fichier. Le trousseau, cependant, fait appel à des clés de classe issues du conteneur de clés de l'utilisateur pour protéger les éléments inclus dans le trousseau de l'utilisateur. Sur les appareils iOS et iPadOS configurés pour un usage par un seul utilisateur (configuration par défaut), le conteneur de clés de l'appareil et celui de l'utilisateur sont un seul et même composant, protégé par le code de l'utilisateur.

Conteneur de clés de sauvegarde

Le conteneur de clés de sauvegarde est créé lorsque le Finder (sous macOS 10.15 ou version ultérieure) ou iTunes (sous macOS 10.14 ou version antérieure) réalise une sauvegarde chiffrée et la stocke sur l'ordinateur sur lequel le contenu de l'appareil est sauvegardé. Un nouveau conteneur de clés est créé avec un nouveau jeu de clés, et les données sauvegardées sont rechiffrées avec ces nouvelles clés. Comme expliqué précédemment, les éléments du trousseau non itinérants restent enveloppés avec la clé extraite de l'UID, ce qui permet de les restaurer sur l'appareil à partir duquel ils ont été initialement sauvegardés, mais les rend inaccessibles sur un autre appareil.

Protégé par le mot de passe configuré, le conteneur de clés est exécuté au fil de 10 millions d'itérations de la fonction de dérivation de clé PBKDF2. Malgré ce grand nombre d'itérations, le conteneur de clés de sauvegarde n'est lié à aucun appareil précis et peut donc théoriquement faire l'objet d'une tentative d'attaque en force exécutée en parallèle sur plusieurs ordinateurs. Cette menace peut être atténuée en utilisant un mot de passe suffisamment robuste.

Si un utilisateur choisit de ne pas chiffrer une sauvegarde, les fichiers ne sont pas chiffrés, quelle que soit la classe de protection des données à laquelle ils appartiennent, mais le trousseau reste protégé par une clé dérivée de l'UID. C'est pourquoi les éléments du trousseau ne peuvent être transférés vers un nouvel appareil que si un mot de passe de sauvegarde est défini.

Conteneur de clés de l'autorité de séquestre

Le conteneur de clés de l'autorité de séquestre est utilisé pour permettre la synchronisation avec le Finder (sous macOS 10.15 ou version ultérieure) ou iTunes (sous macOS 10.14 ou version antérieure) au moyen d'une connexion USB et de la gestion des appareils mobiles (GAM). Ce conteneur de clés permet au Finder ou à iTunes de réaliser des sauvegardes et des synchronisations sans nécessiter la saisie d'un code par l'utilisateur, et à une solution de GAM d'effacer à distance le code d'un utilisateur. Il est stocké sur l'ordinateur utilisé pour effectuer la synchronisation avec le Finder ou iTunes, ou dans la solution de GAM qui gère l'appareil à distance.

Le conteneur de clés de l'autorité de séquestre améliore l'expérience de l'utilisateur lors de la synchronisation de l'appareil, qui peut nécessiter l'accès à toutes les classes de données. Lors de la première connexion au Finder ou à iTunes d'un appareil verrouillé à l'aide d'un code, l'utilisateur est invité à saisir ce dernier. L'appareil crée ensuite un conteneur de clés de l'autorité de séquestre contenant les mêmes clés de classe que celles qu'il utilise et génère une nouvelle clé pour le protéger. Le conteneur de clés de l'autorité de séquestre et la clé qui le protège sont répartis entre l'appareil et l'hôte ou le serveur, les données stockées sur l'appareil étant affectées à la classe « Protection complète jusqu'à la première authentification de l'utilisateur ». C'est pourquoi le code de l'appareil doit être saisi la première fois que l'utilisateur réalise une sauvegarde avec le Finder ou iTunes après un redémarrage.

Dans le cas d'une mise à jour logicielle sans fil, l'utilisateur est invité à saisir son code au lancement de la mise à jour. Cette technique sert à créer de façon sécurisée un jeton de déverrouillage à usage unique qui déverrouille le conteneur de clés de l'utilisateur après la mise à jour. Ce jeton ne peut pas être généré sans saisir le code de l'utilisateur, et tout jeton précédemment généré est invalidé si le code de l'utilisateur a changé entre-temps.

Les jetons de déverrouillage à usage unique sont prévus aussi bien pour l'installation surveillée que pour celle sans surveillance d'une mise à jour logicielle. Ils sont chiffrés à l'aide d'une clé dérivée de la valeur active d'un compteur monotone dans le Secure Enclave, de l'UUID du conteneur de clés et de l'UID du Secure Enclave.

Sur les systèmes sur une puce A9 ou de génération ultérieure, le jeton de déverrouillage à usage unique ne dépend plus des compteurs ou du stockage effaçable. Il est désormais protégé par le nonce antirejeu contrôlé par le Secure Enclave.

Le jeton de déverrouillage à usage unique pour les mises à jour logicielles surveillées expire au bout de 20 minutes. Sous iOS 13 et iPadOS 13.1 ou versions ultérieures, le jeton est stocké dans un casier protégé par le Secure Enclave. Avant iOS 13, ce jeton était exporté à partir du Secure Enclave et écrit dans le stockage effaçable ou était protégé par le mécanisme antirejeu du Secure Enclave. Une minuterie de règlement incrémente le compteur si l'appareil n'a pas redémarré dans les 20 minutes.

Les mises à jour logicielles sans surveillance ont lieu lorsque le système détecte une nouvelle mise à jour et lorsque l'une des conditions suivantes est vérifiée :

- les mises à jour automatiques sont configurées dans iOS 12 ou une version ultérieure;
- l'utilisateur choisit l'option Installer plus tard lorsqu'il est informé de la mise à jour.

Une fois que l'utilisateur saisit son code, un jeton de déverrouillage à usage unique est généré et demeure valide dans le Secure Enclave jusqu'à huit heures. Si la mise à jour n'a pas encore eu lieu, ce jeton de déverrouillage à usage unique est détruit à chaque verrouillage et recréé à chaque déverrouillage ultérieur. Chaque déverrouillage réinitialise le délai de huit heures. Après huit heures, une minuterie de règlement invalide le jeton de déverrouillage à usage unique.

Conteneur de clés de sauvegarde iCloud

Le conteneur de clés de sauvegarde iCloud est similaire au conteneur de clés de sauvegarde. Toutes les clés de classe présentes dans ce conteneur de clés sont asymétriques (chiffrées avec la courbe elliptique Curve25519, comme celles de la classe de protection de données « Protection complète sauf si des données sont ouvertes »). Un conteneur de clés asymétriques est également utilisé pour la sauvegarde dans la fonctionnalité de récupération du trousseau iCloud.

Protection des clés dans d'autres modes de démarrage

La protection des données est conçue pour fournir l'accès aux données utilisateur uniquement après une authentification valide et seulement à l'utilisateur autorisé. Les classes de protection des données se prêtent à divers cas d'utilisation, comme la possibilité de lire et écrire certaines données, même lorsqu'un appareil est verrouillé (mais après le déverrouillage initial). Des mesures supplémentaires sont prises pour protéger l'accès aux données utilisateur lors de l'utilisation d'autres modes de démarrage, comme celles prises avec le mode DFU (Device Firmware Upgrade, mise à niveau du programme interne de l'appareil), avec le mode de récupération, avec l'utilitaire Diagnostic Apple ou pendant les mises à jour logicielles. Ces capacités reposent sur une combinaison de fonctionnalités matérielles et logicielles, et ont été étendues au fil de l'évolution des puces conçues par Apple.

Fonctionnalité	A10	A11, S3	A12, S4	A13, S5	A14, M1, S6
Récupération : Toutes les classes de protection des données sont protégées.	✓	✓	✓	✓	✓
Autres démarrages du mode DFU, de la récupération et des mises à jour logicielles : Les données des classes A, B et C sont protégées.			✓	✓	✓

Le moteur AES du Secure Enclave est équipé de bits de départ de logiciel verrouillables. Lorsque des clés sont créées à partir de l'UID, ces bits de départ sont inclus dans la fonction de dérivation de clé pour générer des hiérarchies de clés supplémentaires. L'utilisation du bit de départ varie selon la puce :

- À partir des systèmes sur une puce A10 et S3 d'Apple, un bit de départ est consacré à la distinction des clés protégées par le code de l'utilisateur. Le bit de départ est réglé pour les clés qui requièrent le code de l'utilisateur (y compris les clés de protection des données de classe A, B et C) et effacé pour celles qui ne l'exigent pas (y compris la clé de métadonnées du système de fichiers et les clés de classe D).

- Sur les appareils dotés d'une puce A10 ou de génération subséquente qui exécutent iOS 13, iPadOS 13.1 ou une version ultérieure de ces systèmes d'exploitation, toutes les données utilisateur sont rendues inaccessibles par chiffrement lorsque les appareils sont démarrés en mode de diagnostic. Pour ce faire, un bit de départ supplémentaire est introduit, dont les réglages gèrent l'accès à la clé de support, elle-même nécessaire pour accéder aux métadonnées (et, par le fait même, au contenu de tous les fichiers) du volume de données chiffré à l'aide de la protection des données. Cette protection couvre tous les fichiers protégés dans les classes (A, B, C et D), pas seulement ceux qui requièrent le code de l'utilisateur.
- Sur les systèmes sur une puce A12, la mémoire morte d'amorçage du Secure Enclave verrouille le bit de départ du code si le processeur d'application passe en mode DFU ou en mode de récupération. Lorsque le bit de départ du code est verrouillé, il est impossible de le modifier, ce qui vise à prévenir l'accès aux données protégées par le code de l'utilisateur.

Restaurer un appareil après qu'il soit passé en mode DFU permet de le remettre en état de bon fonctionnement et d'avoir la certitude qu'il ne contient qu'un code intact signé par Apple. Le mode DFU est accessible manuellement.

Consultez les ressources suivantes de l'assistance Apple sur l'activation du mode DFU sur un appareil :

Appareil	Article
iPhone, iPad, iPod touch	Si vous avez oublié le code d'accès de votre iPhone ou si votre iPhone est désactivé
Apple TV	Restauration de votre Apple TV
Mac avec puce Apple	Relancer ou restaurer un Mac doté d'une puce Apple

Protection des données utilisateur contre les attaques

Les assaillants qui tentent de soustraire des données utilisateur déploient généralement plusieurs techniques : extraire les données chiffrées vers un autre support dans le cadre d'une attaque en force, manipuler la version du système d'exploitation, ou modifier ou affaiblir le règlement de sécurité de l'appareil pour faciliter l'attaque. S'attaquer aux données sur l'appareil requiert le plus souvent de pouvoir communiquer avec lui au moyen d'une interface matérielle, par exemple par un port Lightning ou USB. Les appareils Apple comportent des fonctionnalités pour aider à prévenir de telles attaques.

Les appareils Apple prennent en charge une technologie dénommée *protection scellée des clés (SKP)* qui a pour but de faire en sorte que le matériel cryptographique est rendu inutilisable en dehors de l'appareil, ou qui est utilisée si des manipulations des versions du système d'exploitation ou des réglages de sécurité sont effectuées sans l'autorisation appropriée de l'utilisateur. Cette fonctionnalité *n'est pas* fournie par le Secure Enclave. Elle est plutôt prise en charge par les registres internes qui se trouvent dans une couche inférieure afin de fournir aux clés nécessaires pour déchiffrer les données utilisateur une couche supplémentaire de protection qui est indépendante du Secure Enclave.

Remarque : La technologie SKP est offerte uniquement sur les appareils dotés d'un système sur une puce conçu par Apple.

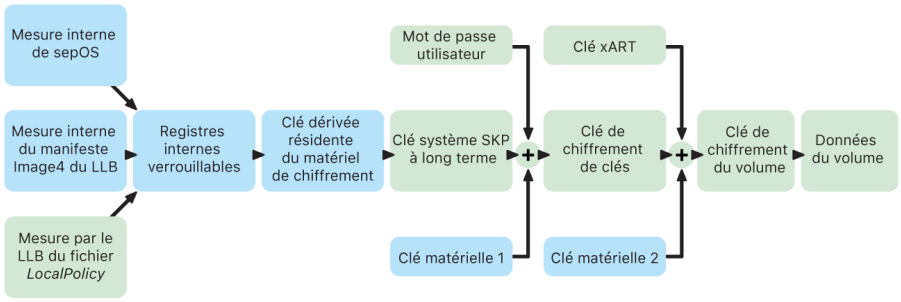
Fonctionnalité	A10	A11, S3	A12, S4	A13, S5	A14, M1, S6
Protection scellée des clés	✓	✓	✓	✓	✓

L'iPhone et l'iPad peuvent aussi être configurés pour activer uniquement les connexions de données dans des conditions qui sont davantage susceptibles d'indiquer que l'appareil est toujours sous le contrôle physique de son propriétaire.

Protection scellée des clés (SKP)

Sur les appareils Apple qui prennent en charge la protection des données, la clé de chiffrement des clés (KEK) est protégée ou scellée par des mesures du logiciel sur le système tout en étant liée à l'UID disponible uniquement auprès du Secure Enclave. Sur un Mac avec puce Apple, la protection de la clé KEK est davantage renforcée en incorporant des informations sur le règlement de sécurité dans le système, car macOS prend en charge les modifications essentielles de ce règlement (telles que la désactivation du démarrage sécurisé ou de la protection de l'intégrité du système) qui ne sont pas prises en charge sur d'autres plateformes. Sur un Mac avec puce Apple, cette protection inclut les clés FileVault, car FileVault est implémenté avec la protection des données (classe C).

La clé qui provient de l'emmêlement du mot de passe de l'utilisateur, de la clé SKP à long terme et de la clé matérielle 1 (l'UID du Secure Enclave) est appelée *clé dérivée du mot de passe*. Cette clé est utilisée pour protéger le conteneur de clés de l'utilisateur (sur toutes les plateformes prises en charge) et la KEK (uniquement sous macOS) et activer le déverrouillage par biométrie ou automatique au moyen d'autres appareils comme l'Apple Watch.



Processus de la protection scellée des clés d'un Mac avec puce Apple.

Le moniteur de démarrage du Secure Enclave capture la mesure du système d'exploitation du Secure Enclave qui est chargé. Lorsque la mémoire morte d'amorçage du processeur d'application mesure le manifeste Image4 joint au LLB, ce manifeste contient alors une mesure de tout autre programme interne couplé au système également chargé. Le fichier LocalPolicy contient les configurations de sécurité centrales chargées pour macOS. Le fichier LocalPolicy contient également le champ `nsih`, un hachage du manifeste Image4 de macOS. Le manifeste Image4 de macOS contient des mesures de l'ensemble des objets de démarrage du programme interne couplé à macOS et de macOS, comme la collection du noyau de démarrage ou le hachage racine du volume système signé (VSS).

Si un assaillant réussit contre toute attente à modifier un des éléments mesurés susmentionnés (programmes internes, logiciels ou composants de la configuration de sécurité), cette modification modifiera à son tour les mesures stockées dans les registres internes. La modification des mesures modifie la valeur de la SMRK (System Measurement Root Key, *clé racine de mesure du système*) dérivée du matériel cryptographique, ce qui brise le sceau de la hiérarchie de clés. La SMDK (system measurement device key, *clé d'appareil de mesure système*) et, par le fait même, la KEK deviennent alors inaccessibles, empêchant ainsi l'assaillant d'accéder aux données.

Cependant, lorsqu'il n'est pas aux prises avec une attaque, le système doit permettre les mises à jour logicielles légitimes qui modifient les mesures du programme interne et le champ `nsih` dans le fichier LocalPolicy pour qu'ils pointent vers de nouvelles mesures de macOS. Avec d'autres systèmes qui essaient d'incorporer des mesures du programme interne, mais qui ne disposent pas d'une source de vérification satisfaisante et reconnue, l'utilisateur doit désactiver le règlement de sécurité, puis mettre à jour le programme interne avant de réactiver le règlement pour capturer une nouvelle mesure de référence. Cela augmente considérablement le risque qu'un assaillant puisse modifier le programme interne pendant une mise à jour logicielle. Le fait que le manifeste Image4 contient toutes les mesures requises contribue à protéger davantage le système. Le matériel qui déchiffre la SMDK avec la SMRK après la validation des mesures au cours d'un démarrage normal peut également chiffrer la SMDK en fonction d'une future SMRK proposée. En spécifiant les mesures attendues après une mise à jour logicielle, le matériel peut chiffrer une SMDK qui est accessible dans un système d'exploitation actuel de manière à ce qu'elle reste accessible dans un système d'exploitation futur. De façon semblable, lorsqu'un utilisateur change légitimement ses réglages de sécurité dans le fichier LocalPolicy, la SMDK doit être chiffrée pour la future SMRK en fonction de la mesure du fichier LocalPolicy que le LLB calculera lors du prochain redémarrage.

Activation sécurisée des connexions de données sous iOS et iPadOS

Sur les appareils iOS ou iPadOS, si aucune connexion de données n'a été récemment établie, les utilisateurs doivent utiliser Touch ID, Face ID ou un code pour activer les connexions de données au moyen d'une interface Lightning, USB ou Smart Connector. Cela limite la surface d'attaque des appareils connectés physiquement tels que des chargeurs malveillants, tout en continuant de permettre l'utilisation d'autres accessoires dans un délai raisonnable. Si plus d'une heure s'est écoulée depuis le verrouillage de l'appareil iOS ou iPadOS, ou depuis la fin de la connexion par l'intermédiaire d'un accessoire, l'appareil n'autorisera l'établissement d'aucune nouvelle connexion avant d'être déverrouillé. Durant cette période d'une heure, seules les connexions provenant d'accessoires qui ont précédemment été connectés à l'appareil pendant qu'il était déverrouillé sont autorisées. Ces accessoires restent en mémoire pour une durée de 30 jours suivant leur dernière connexion. Si un accessoire inconnu tente d'établir une connexion avec les données pendant cette période, toutes les connexions d'accessoires par Lightning, USB et Smart Connector sont désactivées jusqu'à ce que l'appareil soit de nouveau déverrouillé. Cette période d'une heure :

- contribue à garantir que les utilisateurs qui se connectent fréquemment par fil à un Mac, à un PC, à des accessoires ou à CarPlay n'auront pas à saisir leur code chaque fois;
- est nécessaire, car l'écosystème d'accessoires n'offre pas un moyen fiable d'identifier les accessoires de manière cryptographique avant d'établir une connexion de données.

Par ailleurs, si plus de trois jours se sont écoulés depuis l'établissement d'une connexion avec un accessoire, l'appareil interdira les nouvelles connexions dès son verrouillage, ce qui a pour but de mieux protéger les utilisateurs qui ne se servent pas souvent de tels accessoires. Les connexions par l'intermédiaire d'accessoires Lightning, USB et Smart Connector sont également désactivées quand la saisie du code est nécessaire pour réactiver l'authentification biométrique.

L'utilisateur peut choisir de réactiver les connexions de données permanentes dans Réglages (la configuration de certains dispositifs d'assistance le fait automatiquement).

Rôle du système de fichiers d'Apple

Le système de fichiers d'Apple (APFS) est un système de fichiers exclusif pensé pour le chiffrement. L'APFS fonctionne sur toutes les plateformes d'Apple : iPhone, iPad, iPod touch, Mac, Apple TV et Apple Watch. Optimisé pour le stockage flash/SSD, il propose un chiffrement complexe, la copie à l'écriture pour les métadonnées, le partage d'espace, le clonage de fichiers et de répertoires, des instantanés, le calcul rapide des tailles de répertoires, le renommage atomique et une amélioration des fondations du système de fichiers, ainsi qu'une conception unique par copie à l'écriture, qui rassemble les opérations afin d'offrir des performances optimales tout en assurant la fiabilité des données.

Partage d'espace

L'APFS alloue de l'espace disque sur demande. Lorsqu'un conteneur APFS est divisé en plusieurs volumes, l'espace libre qu'il renferme peut être attribué à n'importe lequel de ces volumes, en fonction des besoins. Comme chaque volume n'utilise qu'une partie du conteneur, l'espace disponible équivaut à la taille du conteneur, moins l'espace total utilisé par ses volumes.

Volumes multiples

Sous macOS 10.15 ou version ultérieure, un conteneur APFS utilisé pour démarrer le Mac doit contenir au moins cinq volumes, dont les trois premiers sont invisibles pour l'utilisateur :

- *volume de prédémarrage :* contient les données nécessaires au démarrage de chaque volume système du conteneur;
- *volume de mémoire virtuelle :* contient les fichiers d'échange sous macOS;
- *volume de secours :* contient recoveryOS;
- *Volume système :* contient :
  - tous les fichiers nécessaires pour démarrer le Mac;
  - toutes les apps installées nativement par macOS (celles qui se trouvaient auparavant dans le dossier /Applications sont maintenant dans le dossier /Système/Applications);

  Remarque : Par défaut, aucun processus ne peut écrire sur le volume système, même les processus système d'Apple.
- *Volume de données :* contient les données susceptibles de changer, comme :
  - toutes données dans le dossier de l'utilisateur, y compris les photos, la musique, les vidéos et les documents;

- les apps installées par l'utilisateur, y compris AppleScript, et les applications Automator;
- les cadres et les démons personnalisés installés par l'utilisateur, par l'entreprise ou par des apps tierces;
- d'autres emplacements inscriptibles dont l'utilisateur est propriétaire, comme /Applications, /Library, /Users, /Volumes, /usr/local, /private, /var et /tmp.

Un volume de données est créé pour chaque volume système supplémentaire. Les volumes de prédémarrage, de mémoire virtuelle et de secours sont tous partagés et ne sont pas dupliqués.

Sous macOS 11, le volume système est capturé dans un instantané. Le système d'exploitation démarre à partir d'un instantané du volume système, et non à partir du montage en lecture seule du volume système mutable.

Sous iOS et iPadOS, le stockage est divisé en au moins deux volumes APFS :

- Volume système
- Volume de données

Protection des données du trousseau

De nombreuses apps doivent traiter des mots de passe et d'autres petits fragments de données confidentielles, comme des clés et des jetons de connexion. Le trousseau offre un moyen sûr de stocker ces éléments. Les systèmes d'exploitation Apple utilisent divers mécanismes pour appliquer les garanties associées aux différentes classes de protection du trousseau. Sous macOS (y compris un Mac avec puce Apple), la protection des données n'est pas directement utilisée pour appliquer ces garanties.

Aperçu

Les éléments du trousseau sont chiffrés avec deux clés AES-256-GCM distinctes : une clé de table (métadonnées) et une clé par rangée (clé secrète). Les métadonnées du trousseau (tous les attributs autres que kSecValue) sont chiffrées avec la clé de métadonnées pour accélérer les recherches, et la valeur secrète (kSecValueData) est chiffrée avec la clé secrète. La clé de métadonnées est protégée par le Secure Enclave, mais elle est mise en cache dans le processeur d'application afin de permettre les interrogations rapides du trousseau. La clé secrète requiert toujours un aller-retour par le Secure Enclave.

Le trousseau utilise une base de données SQLite stockée sur le système de fichiers. Il n'y a qu'une seule base de données, et le démon `securityd` détermine les éléments du trousseau auxquels chaque processus ou app peut accéder. Les API d'accès au trousseau envoient des appels au démon, lequel interroge les autorisations « groupes d'accès au trousseau », « identifiant d'application » et « groupe d'applications » de l'app. Au lieu de limiter l'accès à un seul processus, les groupes d'accès permettent de partager les éléments du trousseau entre les apps.

Les éléments du trousseau ne peuvent être partagés qu'entre les apps du même développeur. Pour partager des éléments du trousseau, les apps tierces utilisent des groupes d'accès portant un préfixe qui leur est alloué par le programme Apple pour les développeurs dans leurs groupes d'applications. L'obligation d'utiliser un préfixe et le caractère unique du groupe d'applications sont contrôlés par la signature du code, les profils d'approvisionnement et le programme Apple pour les développeurs.

Les données du trousseau sont protégées à l'aide d'une structure de classes similaire à celle utilisée pour la protection des données des fichiers. Ces classes présentent des comportements équivalents aux classes de protection des données des fichiers, mais les clés et les fonctions qu'elles utilisent sont différentes.

Disponibilité	Protection des données des fichiers	Protection des données du trousseau
Lorsque l'appareil est déverrouillé	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
Lorsque l'appareil est verrouillé	NSFileProtectionCompleteUnless Open	S. O.
Après le premier déverrouillage	NSFileProtectionCompleteUntil FirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Toujours	NSFileProtectionNone	kSecAttrAccessibleAlways
Code activé	S. O.	kSecAttrAccessibleWhenPasscode SetThisDeviceOnly

Les apps qui font appel à des services d'actualisation en arrière-plan peuvent utiliser la classe *kSecAttrAccessibleAfterFirstUnlock* pour les éléments du trousseau qui doivent être accessibles lors des mises à jour en arrière-plan.

La classe *kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly* se comporte comme la classe *kSecAttrAccessibleWhenUnlocked*, mais n'est disponible que si un code est configuré pour l'appareil. Cette classe n'existe que dans le conteneur de clés du système. Ces éléments :

- ne se synchronisent pas avec le trousseau iCloud;
- ne sont pas sauvegardés;
- ne sont pas inclus dans les conteneurs de clés de l'autorité de séquestre.

Si le code est supprimé ou réinitialisé, les éléments sont rendus inutilisables par l'effacement des clés de classe.

D'autres classes du trousseau ont un pendant « Cet appareil uniquement », qui est toujours protégé par l'UID quand il est copié à partir de l'appareil lors d'une sauvegarde, ce qui le rend inutilisable s'il est restauré sur un autre appareil. Apple a pris soin de trouver un juste équilibre entre sécurité et convivialité en choisissant les classes du trousseau qui dépendent du type d'informations sécurisées et en définissant quand elles sont requises par iOS et iPadOS. Par exemple, un certificat VPN doit toujours être disponible pour que l'appareil puisse rester connecté en permanence, mais il est classé comme élément « non itinérant » et ne peut donc pas être transféré vers un autre appareil.

Protections des classes de données du trousseau

Les protections des classes mentionnées ci-dessous sont imposées pour les éléments du trousseau.

Élément	Accessible
Mots de passe Wi-Fi	Après le premier déverrouillage

Élément	Accessible
Comptes Mail	Après le premier déverrouillage
Comptes Microsoft Exchange ActiveSync	Après le premier déverrouillage
Mots de passe VPN	Après le premier déverrouillage
LDAP, CalDAV, CardDAV	Après le premier déverrouillage
Jetons des comptes de réseau social	Après le premier déverrouillage
Clés de chiffrement des notifications Handoff	Après le premier déverrouillage
Jeton iCloud	Après le premier déverrouillage
Clés iMessage	Après le premier déverrouillage
Mot de passe de partage à domicile	Lorsque l'appareil est déverrouillé
Mots de passe Safari	Lorsque l'appareil est déverrouillé
Signets Safari	Lorsque l'appareil est déverrouillé
Sauvegarde par le Finder ou iTunes	Non itinérant lorsque l'appareil est déverrouillé
Certificats VPN	Non itinérant en toute circonstance
Clés Bluetooth®	Non itinérant en toute circonstance
Jeton du service de notifications Push d'Apple (APN)	Non itinérant en toute circonstance
Certificats et clé privée iCloud	Non itinérant en toute circonstance
Certificats et clés privées installés par un profil de configuration	Non itinérant en toute circonstance
NIP de la carte SIM	Non itinérant en toute circonstance
Jeton Localiser	Toujours
Messagerie	Toujours

Contrôle de l'accès au trousseau

Les trousseaux peuvent utiliser des listes de contrôle d'accès (ACL, Access Control List) pour définir des règles précisant les conditions d'accessibilité et d'authentification. Les éléments peuvent établir des conditions nécessitant la présence de l'utilisateur en spécifiant qu'ils ne sont accessibles que si celui-ci s'authentifie à l'aide de Touch ID ou Face ID, ou en saisissant le code de ou le mot de passe de l'appareil. Il est aussi possible de limiter l'accès aux éléments en indiquant que l'inscription Touch ID ou Face ID n'a pas changé depuis l'ajout de l'élément. Cette limite contribue à empêcher un assaillant d'ajouter sa propre empreinte digitale dans le but d'accéder à un élément du trousseau. Les listes ACL sont évaluées à l'intérieur du Secure Enclave et ne sont transmises au noyau que si les conditions définies sont remplies.

Architecture du trousseau sous macOS

macOS donne accès au trousseau pour stocker de façon pratique et sécurisée les noms d'utilisateur et les mots de passe, les identités numériques, les clés de chiffrement et les notes sécurisées. Le trousseau est accessible par l'app Trousseaux d'accès dans /Applications/Utilitaires/. Grâce à lui, l'utilisateur n'a pas à saisir d'informations d'identification, ni même à les mémoriser. Un premier trousseau par défaut est créé pour chaque utilisateur du Mac, et il est possible d'en ajouter d'autres pour des besoins précis.

En plus de compter sur les trousseaux d'utilisateur, macOS fait appel à plusieurs trousseaux système pour consigner les éléments d'authentification qui ne sont pas liés à un utilisateur, comme les informations d'identification réseau et les identités d'infrastructure à clés publiques (ICP). Un de ces trousseaux, Racines du système, est immuable et contient les certificats des autorités de certification racine d'ICP Internet pour permettre l'exécution de tâches courantes telles que les services bancaires et les transactions en ligne. De même, l'utilisateur peut déployer des certificats de l'autorité de certification fournis à l'interne aux ordinateurs Mac gérés pour contribuer à la validation de sites et de services internes.

FileVault

Chiffrement de volumes avec FileVault sous macOS

Les ordinateurs Mac proposent FileVault, une fonctionnalité de chiffrement intégrée pour sécuriser toutes les données au repos. FileVault utilise l'algorithme de chiffrement de données AES-XTS pour protéger l'intégralité des volumes sur les dispositifs de stockage internes et amovibles.

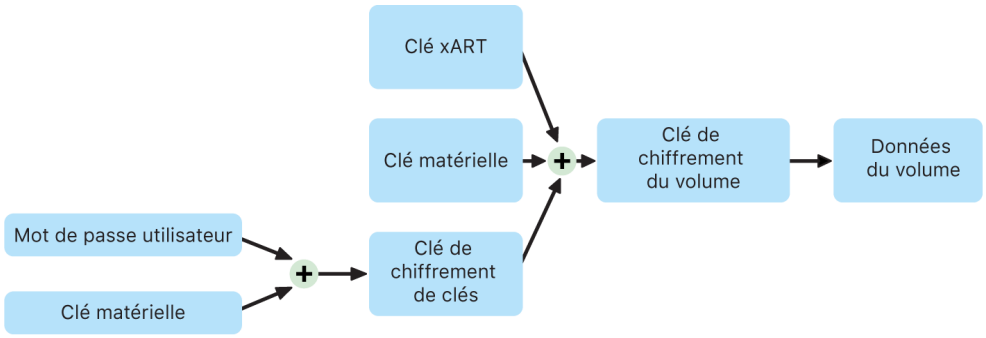
FileVault sur un Mac avec puce Apple est en fait implémenté par la classe C de protection des données au moyen d'une clé de volume. Sur un Mac doté de la puce T2 Security d'Apple ainsi que sur un Mac avec puce Apple, les dispositifs de stockage internes chiffrés qui sont directement connectés au Secure Enclave tirent profit des fonctionnalités de sécurité matérielles de ce dernier et du moteur AES. Après l'activation de FileVault sur un Mac, les informations d'identification de l'utilisateur sont requises au démarrage.

Stockage interne avec FileVault activé

Si l'utilisateur ne fournit pas les bonnes informations d'identification ou la clé de secours cryptographique, les volumes APFS internes demeurent chiffrés et protégés contre les accès non autorisés, même si le dispositif de stockage est retiré du Mac et branché à un autre ordinateur. Sous macOS 10.15, cela inclut le volume système et le volume de données. À partir de macOS 11, le volume système est protégé par la fonctionnalité de volume système signé (VSS), mais le volume de données reste protégé par la solution de chiffrement. Le chiffrement des volumes internes sur un Mac doté d'une puce Apple ou de la puce T2 est mis en œuvre par l'élaboration et la gestion d'une hiérarchie de clés, et repose sur les technologies de chiffrement matériel intégrées à la puce. Cette hiérarchie de clés est conçue pour réaliser simultanément quatre objectifs :

- exiger le mot de passe de l'utilisateur pour le déchiffrement;
- protéger le système contre une attaque en force visant directement des supports de stockage retirés du Mac;

- fournir une méthode rapide et sécurisée pour effacer le contenu par la suppression du matériel cryptographique nécessaire;
- autoriser les utilisateurs à modifier leur mot de passe (puis les clés cryptographiques utilisées pour protéger leurs fichiers) sans devoir chiffrer à nouveau l'intégralité du volume.

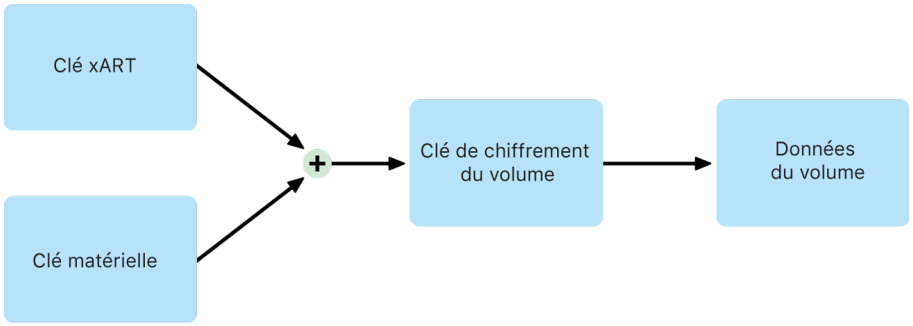


Chiffrement des volumes internes lorsque FileVault est activé sous macOS.

Sur un Mac doté d'une puce Apple ou de la puce T2, toute la gestion des clés de FileVault se produit dans le Secure Enclave; les clés de chiffrement ne sont jamais directement exposées au processeur Intel. Tous les volumes APFS sont créés avec une clé de chiffrement de volume par défaut. Le contenu des volumes et des métadonnées est chiffré à l'aide de cette clé de chiffrement de volume, qui est enveloppée à l'aide de la clé de classe. La clé de classe est protégée par une combinaison du mot de passe de l'utilisateur et de l'UID de l'appareil lorsque FileVault est activé.

Stockage interne avec FileVault désactivé

Si FileVault n'est pas activé sur un Mac doté d'une puce Apple ou de la puce T2 au cours du processus initial d'Assistant réglages, le volume est quand même chiffré, mais la clé de chiffrement de volume est protégée uniquement par l'UID de l'appareil dans le Secure Enclave.



Chiffrement des volumes internes lorsque FileVault est désactivé sous macOS.

Si FileVault est activé plus tard (un processus immédiat puisque les données sont déjà chiffrées), un mécanisme antirejeu contribue à empêcher l'ancienne clé (basée uniquement sur l'UID de l'appareil) d'être utilisée pour déchiffrer le volume. Le volume est ensuite protégé par une combinaison du mot de passe de l'utilisateur et de l'UID de l'appareil conformément aux explications précédentes.

Suppression des volumes FileVault

À la suppression d'un volume, la clé de chiffrement du volume est supprimée de façon sécurisée par le Secure Enclave, ce qui contribue à empêcher cette clé d'être utilisée ultérieurement, même par le Secure Enclave. De plus, toutes les clés de chiffrement de volume sont enveloppées à l'aide d'une clé de support. Cette clé ne renforce pas la confidentialité des données. Elle est plutôt conçue pour permettre la suppression rapide et sécurisée des données. En son absence, le déchiffrement est impossible.

Sur un Mac doté d'une puce Apple ou de la puce T2, la suppression de la clé de support est garantie par la technologie prise en charge par le Secure Enclave, par exemple au moyen de commandes de GAM à distance. Effacer la clé de support de cette manière rend impossible le déchiffrement du volume.

Dispositifs de stockage amovibles

Le chiffrement des dispositifs de stockage amovibles n'utilise pas les capacités de sécurité du Secure Enclave; il est effectué de la même façon que sur un Mac avec processeur Intel sans puce T2.

Gestion de FileVault sous macOS

Utilisation de jetons sécurisés

Le système de fichiers d'Apple (APFS) sous macOS 10.13 et les versions ultérieures change la façon dont les clés de chiffrement FileVault sont générées. Sous les versions précédentes de macOS sur les volumes Core Storage, les clés utilisées dans le processus de chiffrement FileVault étaient créées lorsqu'un utilisateur ou une entreprise activait FileVault sur un Mac. Sous macOS sur les volumes APFS, les clés sont générées soit lors de la création de l'utilisateur, en configurant le mot de passe du premier utilisateur, soit lors de la première connexion d'un utilisateur du Mac. Cette implémentation des clés de chiffrement, le moment où elles sont générées et la façon dont elles sont stockées font partie d'une fonctionnalité appelée *jeton sécurisé*. Plus précisément, un jeton sécurisé est une version enveloppée d'une clé de chiffrement de clés (KEK) protégée par le mot de passe d'un utilisateur.

Lors du déploiement de FileVault dans l'APFS, l'utilisateur peut continuer à :

- utiliser les outils et les processus existants, comme une clé de secours personnelle qui peut être stockée dans une solution de gestion des appareils mobiles (GAM) pour l'autorité de séquestre;
- créer et utiliser une clé de secours institutionnelle;
- reporter l'activation de FileVault jusqu'à la connexion ou la déconnexion d'un utilisateur du Mac.

Sous macOS 11, la configuration initiale du mot de passe du premier utilisateur d'un Mac entraîne l'attribution à cet utilisateur d'un jeton sécurisé. Dans certains cas, ce processus pourrait ne pas être souhaité, car l'attribution du premier jeton de sécurité requiert la connexion au compte utilisateur. Pour empêcher ce cas de figure, ajoutez `;DisabledTags;SecureToken` à l'attribut `AuthenticationAuthority` de l'utilisateur qui a été créé de façon programmée avant de configurer le mot de passe de l'utilisateur, comme indiqué ci-dessous :

```
sudo dscl . append /Users/<user name> AuthenticationAuthority
";DisabledTags;SecureToken"
```

Utilisation du jeton d'amorçage

macOS 10.15 a introduit une nouvelle fonctionnalité, le jeton d'amorçage, pour faciliter l'attribution d'un jeton sécurisé aux comptes mobiles et au compte administrateur facultatif créé par l'inscription de l'appareil (« administrateur géré »). Dans macOS 11, le jeton d'amorçage peut attribuer un jeton sécurisé à tout utilisateur se connectant à l'ordinateur Mac, y compris à des comptes utilisateur locaux. L'utilisation de la fonctionnalité du jeton d'amorçage de macOS 10.15 ou version ultérieure requiert :

- l'inscription du Mac à la solution de GAM par l'entremise d'Apple School Manager ou d'Apple Business Manager, ce qui rend le Mac supervisé;
- le soutien du fournisseur de solution de GAM.

Sous macOS 10.15.4 et les versions ultérieures, un jeton d'amorçage est généré et envoyé à l'autorité de séquestre dans la solution de GAM lors de la première connexion de tout utilisateur pour lequel le jeton sécurisé est activé si cette fonctionnalité est prise en charge par la solution de GAM. Un jeton d'amorçage peut être généré et envoyé à l'autorité de séquestre dans la solution de GAM à l'aide de l'outil de ligne de commande `profiles`, au besoin.

Sous macOS 11, le jeton d'amorçage peut également être utilisé dans d'autres cas de figure, et non pas seulement pour attribuer des jetons sécurisés aux comptes utilisateur. Sur un Mac avec puce Apple, le jeton d'amorçage, si disponible, peut être utilisé pour autoriser l'installation d'extensions de noyau et de mises à jour logicielles lorsque les Mac sont gérés au moyen de la solution de GAM.

Apple et la protection des données personnelles

Protections contre l'accès des apps aux données utilisateur

En plus de chiffrer les données au repos, les appareils Apple empêchent les apps d'accéder aux données personnelles de l'utilisateur sans permission à l'aide de différentes technologies, notamment Data Vault. Dans Réglages sous iOS et iPadOS, ou Préférences Système sous macOS, l'utilisateur peut voir quelles apps sont autorisées à accéder à certaines données, ainsi qu'autoriser ou refuser tout accès ultérieur. L'accès est contrôlé dans les éléments suivants :

- *iOS, iPadOS et macOS :* Calendrier, Appareil photo, Contacts, Micro, Photos, Rappels, Reconnaissance vocale
- *iOS et iPadOS :* Bluetooth, Domicile, Contenu multimédia, Média et Apple Music, Mouvements et forme
- *iOS et watchOS :* Santé
- *macOS :* Surveillance des entrées (par exemple frappes de clavier), Invite, Enregistrement d'écran (par exemple captures d'écran statiques et vidéos), Préférences Système

Sous iOS 13.4 et iPadOS 13.4, ou les versions ultérieures, les données de toutes les apps tierces sont automatiquement protégées par Data Vault. Cette précaution prévient tout accès non autorisé aux données, même par des processus qui ne sont pas mis en bac à sable.

Si l'utilisateur se connecte à iCloud, les apps sous iOS et iPadOS obtiennent par défaut l'accès à iCloud Drive. Les utilisateurs peuvent contrôler l'accès de chaque app dans les réglages d'iCloud. iOS et iPadOS fournissent également des restrictions visant à interdire tout mouvement de données entre les apps et les comptes installés par une solution de gestion des appareils mobiles (GAM) et ceux installés par l'utilisateur.

Protection de l'accès aux données médicales de l'utilisateur

HealthKit fournit un référentiel central destiné aux données de santé et de mise en forme sur iPhone et Apple Watch. HealthKit fonctionne aussi directement avec les appareils de santé et de mise en forme, comme les moniteurs de fréquence cardiaque Bluetooth faible énergie (BLE) compatibles et le coprocesseur de mouvement intégré à de nombreux appareils iOS. Toute interaction de HealthKit avec les apps ou les appareils de santé et de mise en forme et les établissements de soins de santé exige l'autorisation de l'utilisateur. Ces données sont associées à la classe de protection des données « Protection complète sauf si des données sont ouvertes ». L'accès aux données est abandonné 10 minutes après le verrouillage de l'appareil et les données redeviennent accessibles la prochaine fois que l'utilisateur saisit son code ou qu'il utilise Touch ID ou Face ID pour le déverrouiller.

Collecte et stockage des données de santé et de mise en forme

HealthKit collecte et stocke également les données de gestion, comme les autorisations d'accès des apps, les noms des appareils connectés à HealthKit et les informations de programmation utilisées pour lancer les apps lorsque de nouvelles données sont disponibles. Ces données sont stockées dans la classe de protection des données « Protection complète jusqu'à la première authentification de l'utilisateur ». Des fichiers journaux temporaires stockent les informations de santé générées pendant que l'appareil est verrouillé, comme lorsque l'utilisateur pratique une activité physique. Ils sont associés à la classe de protection des données « Protection complète sauf si des données sont ouvertes ». Lorsque l'appareil est déverrouillé, les fichiers journaux temporaires sont importés dans les bases de données médicales principales, puis supprimés une fois la fusion terminée.

Les données médicales peuvent être stockées sur iCloud. Le chiffrement de bout en bout des données médicales requiert iOS 12 ou une version ultérieure ainsi que l'authentification à deux facteurs. Autrement, les données de l'utilisateur sont quand même chiffrées lors du stockage et de la transmission, mais elles ne sont pas chiffrées de bout en bout. Après l'activation de l'authentification à deux facteurs et la mise à niveau vers iOS 12 ou une version ultérieure, les données médicales de l'utilisateur utilisent le chiffrement de bout en bout.

Si l'utilisateur effectue la sauvegarde de son appareil avec le Finder (sous macOS 10.15 ou une version ultérieure) ou iTunes (macOS 10.14 ou une version antérieure), les données médicales sont stockées uniquement si la sauvegarde est chiffrée.

Dossiers médicaux

Les utilisateurs peuvent se connecter aux systèmes de santé compatibles dans l'app Santé pour obtenir une copie de leurs dossiers médicaux. Lorsqu'il se connecte à un système de santé, l'utilisateur s'authentifie en utilisant ses informations d'identification de client OAuth 2. Une fois la connexion établie, les données des dossiers médicaux sont téléchargées directement auprès de l'établissement de soins de santé par une connexion protégée TLS 1.3. Après le téléchargement, les dossiers médicaux sont stockés de façon sécurisée avec les autres données médicales.

Intégrité des données médicales

Les données stockées dans la base de données comprennent des métadonnées permettant de connaître la provenance de chaque enregistrement. Ces métadonnées incluent un identifiant d'app qui identifie l'app ayant stocké l'enregistrement. En outre, un élément de métadonnées facultatif peut contenir une copie signée numériquement de l'enregistrement afin d'assurer l'intégrité des données des enregistrements générés par un appareil approuvé. Le format utilisé pour la signature numérique est la syntaxe de message cryptographique (CMS) spécifiée dans la norme RFC 5652.

Accès aux données médicales par les apps tierces

L'accès à l'API HealthKit est contrôlé par des déclarations d'autorisation, et les apps doivent se conformer aux restrictions concernant l'utilisation des données. Par exemple, elles ne sont pas autorisées à utiliser les données médicales pour afficher des publicités. Elles doivent également fournir aux utilisateurs une politique de confidentialité indiquant en détail comment elles utilisent les données médicales.

L'accès aux données médicales par les apps est contrôlé par les réglages de confidentialité de l'utilisateur. Lorsque des apps demandent à accéder aux données médicales, l'utilisateur est invité à indiquer son choix, comme pour Contacts, Photos et d'autres sources de données iOS. Toutefois, pour les données médicales, les apps se voient accorder des accès distincts pour la lecture et l'écriture ainsi que pour chaque type de données médicales. Les utilisateurs peuvent consulter et révoquer les autorisations d'accès aux données médicales qu'ils ont accordées sous Réglages > Santé > Accès aux données et appareils.

Si des apps sont autorisées à écrire des données, elles peuvent également lire celles-ci. Si elles sont autorisées à lire des données, les apps peuvent lire les données écrites par toutes les sources. Toutefois, les apps ne peuvent pas déterminer les autorisations d'accès accordées aux autres apps. En outre, elles ne peuvent pas savoir avec certitude si elles sont autorisées à lire les données médicales. Quand une app ne dispose pas d'une autorisation de lecture, les requêtes ne renvoient aucune donnée, comme lorsque la base de données est vide. Cela vise à empêcher les apps de déduire l'état de santé de l'utilisateur à partir des types de données qui l'intéressent.

Fiche médicale pour les utilisateurs

L'app Santé offre aux utilisateurs la possibilité de remplir une fiche médicale avec des informations qui pourraient s'avérer importantes en cas d'urgence. Celles-ci sont saisies ou actualisées manuellement et ne sont pas synchronisées avec les informations contenues dans les bases de données médicales.

Les informations de la fiche médicale peuvent être consultées en touchant le bouton Urgence sur l'écran verrouillé. Elles sont stockées sur l'appareil avec la classe de protection des données « Aucune protection » afin d'être accessibles sans avoir à saisir le code de l'appareil. La fiche médicale est une fonctionnalité facultative qui permet aux utilisateurs de trouver un juste équilibre entre sécurité et confidentialité. Ces données sont sauvegardées dans la sauvegarde iCloud sous iOS 13 ou version antérieure. Dans iOS 14, la fiche médicale est synchronisée entre les appareils au moyen de CloudKit et présente les mêmes caractéristiques de chiffrement que le reste des données médicales.

Signature numérique et chiffrement

Listes de contrôle d'accès

Comme les données du trousseau sont partitionnées et protégées par des listes de contrôle d'accès, les informations d'identification stockées par des apps tierces ne peuvent pas être obtenues par des apps présentant une autre identité, à moins que l'utilisateur n'autorise expressément leur transmission. Ce mécanisme permet de sécuriser, sur les appareils Apple, les informations d'identification dans plusieurs apps et services au sein d'une entreprise.

Mail

Dans l'app Mail, les utilisateurs peuvent envoyer des messages signés numériquement et chiffrés. Mail détecte automatiquement les adresses courriel sensibles à la casse et les noms alternatifs répondant à la norme RFC 5322 sur les certificats de chiffrement et de signature numériques sur les jetons de vérification de l'identité personnelle (PIV, Personal Identity Verification) contenus dans les cartes intelligentes compatibles. Si un compte de courriel configuré correspond à une adresse courriel contenue dans une signature numérique ou un certificat de chiffrement sur un jeton PIV joint, Mail affiche automatiquement le bouton de signature dans la barre d'outils de la fenêtre d'un nouveau message. Si Mail dispose du certificat de chiffrement du destinataire, ou si elle peut le repérer dans la liste d'adresses globale (LAG) de Microsoft Exchange, une icône de cadenas déverrouillé apparaît dans la barre d'outils d'un nouveau message. L'icône de cadenas verrouillé indique que le contenu du message envoyé sera chiffré à l'aide de la clé publique du destinataire.

Chiffrement par message S/MIME

iOS, iPadOS et macOS prennent en charge le chiffrement par message S/MIME. Les utilisateurs de S/MIME peuvent donc choisir de signer et de chiffrer tous leurs messages par défaut, ou certains messages seulement.

Les identités utilisées avec le chiffrement S/MIME peuvent être envoyées aux appareils Apple à l'aide d'un profil de configuration, d'une solution de gestion des appareils mobiles (GAM), du protocole Simple Certificate Enrollment Protocol (SCEP) ou de l'autorité de certification Microsoft Active Directory.

Cartes intelligentes

macOS 10.12 et les versions ultérieures assurent la prise en charge native des cartes de vérification de l'identité personnelle (PIV). L'utilisation de ces cartes est très répandue au sein des organisations commerciales et gouvernementales pour l'authentification à deux facteurs, la signature numérique et le chiffrement.

Les cartes intelligentes contiennent au moins une identité numérique dotée d'une paire de clés publique et privée, et d'un certificat associé. Le déverrouillage d'une carte intelligente à l'aide du numéro d'identification personnel (NIP) donne accès aux clés privées utilisées pour les opérations d'authentification, de chiffrement et de signature. Le certificat détermine à quelles fins la clé peut être utilisée, quels attributs y sont associés, et si elle est validée (signée) par une autorité de certification (AC).

Les cartes intelligentes peuvent être utilisées pour l'authentification à deux facteurs. Les deux facteurs requis pour déverrouiller une carte comprennent un élément que l'utilisateur possède (la carte) et un élément que l'utilisateur connaît (le NIP). macOS 10.12 et les versions ultérieures assurent également la prise en charge native de l'authentification par carte intelligente à partir de la fenêtre d'ouverture de session, ainsi que de l'authentification par certificat client sur les sites Web dans Safari. Ces systèmes d'exploitation prennent aussi en charge le protocole Kerberos à l'aide de biclés (PKINIT) pour la connexion par signature unique aux services compatibles avec ce protocole. Pour en savoir plus sur les cartes intelligentes et macOS, consultez l'introduction à l'intégration des cartes intelligentes de la *Référence de déploiement pour Mac*.

Images disques chiffrées

Sous macOS, les images disques chiffrées servent de conteneurs sécurisés dans lesquels les utilisateurs peuvent stocker ou transférer des documents confidentiels et d'autres fichiers. Elles sont créées avec Utilitaire de disque (situé dans Applications/Utilitaires/) et peuvent être chiffrées par AES 128 bits ou 256 bits. Puisqu'une image disque montée est traitée comme un volume local connecté à un Mac, les utilisateurs peuvent copier, déplacer et ouvrir les fichiers et dossiers qu'elle contient. Comme avec FileVault, le contenu d'une image disque est chiffré et déchiffré en temps réel. Les utilisateurs peuvent échanger en toute sécurité des documents, fichiers et dossiers en sauvegardant une image disque chiffrée sur un support amovible, en l'envoyant par courriel sous forme de pièce jointe ou en la stockant sur un serveur distant. Pour en savoir plus sur les images disques chiffrées, consultez le Guide de l'utilisateur d'Utilitaire de disque.

Sécurité des apps

Aperçu de la sécurité des apps

Aujourd'hui, les apps sont parmi les éléments les plus importants d'une architecture de sécurité. Elles sont de formidables outils de productivité, mais si elles ne sont pas gérées adéquatement, elles peuvent potentiellement nuire à la sécurité et à la stabilité du système et mettre les données des utilisateurs en péril.

Pour cette raison, Apple met en place des couches de protection servant à vérifier que les apps ne comportent pas de programmes malveillants connus et qu'elles n'ont pas été altérées. Et d'autres mesures permettent de contrôler rigoureusement l'accès des apps aux données de l'utilisateur. Ces contrôles de sécurité offrent une plateforme stable et sûre pour les apps, ce qui permet aux développeurs de proposer des centaines de milliers d'apps pour iOS, iPadOS et macOS – le tout sans compromettre l'intégrité du système. Les utilisateurs peuvent ensuite accéder à ces apps sur des appareils Apple sans craindre outre mesure les virus, les logiciels malveillants et les autres types d'attaques.

Sur iPhone, iPad et iPod touch, toutes les apps proviennent de l'App Store (et sont mises en bac à sable) pour garantir un contrôle serré.

Sur Mac, de nombreuses apps sont obtenues par l'entremise l'App Store, mais les utilisateurs peuvent également télécharger et installer des logiciels provenant d'Internet. Pour rendre ces téléchargements plus sûrs, macOS dispose de contrôles supplémentaires. Tout d'abord, sous macOS 10.15 et les versions ultérieures, toutes les apps doivent être notarisées par Apple pour que leur exécution soit autorisée. Cette exigence vise à prévenir la présence de logiciels malveillants connus dans les apps lorsque celles-ci ne sont pas obtenues sur l'App Store. macOS inclut également une protection antivirus de pointe pour bloquer et, au besoin, supprimer tout logiciel malveillant.

La mise en bac à sable assure un contrôle complémentaire sur l'ensemble des plateformes en protégeant les données des utilisateurs de tout accès non autorisé par les apps. Et sous macOS, les données essentielles sont elles aussi protégées. Ainsi, que les apps qui tentent d'y accéder soient elles-mêmes mises en bac à sable ou non, les utilisateurs demeurent maîtres de l'accès à leurs fichiers, notamment sur le Bureau et dans les dossiers Documents et Téléchargements.

Fonctionnalité native	Équivalent tiers
Liste des modules non approuvés, liste des extensions Safari non approuvées	Définitions de logiciels malveillants ou de virus
Quarantaine de fichiers	Définitions de logiciels malveillants ou de virus

Fonctionnalité native	Équivalent tiers
Signatures XProtect ou YARA	Définitions de logiciels malveillants ou de virus
Outil de suppression de logiciels malveillants	Protection des terminaux
Gatekeeper	Protection des terminaux; elle applique la signature du code sur les apps afin de contribuer à garantir que seuls les logiciels fiables soient exécutés.
eficheck (nécessaire pour un Mac sans puce T2 Security d'Apple)	Protection des terminaux; détection des trousses administrateur pirate
Coupe-feu d'application	Protection des terminaux; coupe-feu
Filtre de paquets	Solutions de coupe-feu
Protection de l'intégrité du système	Intégrée à macOS
Contrôles d'accès obligatoires	Intégrés à macOS
Liste d'exclusion des extensions du noyau	Intégrée à macOS
Signature obligatoire du code des apps	Intégrée à macOS
Notarisation des apps	Intégrée à macOS

Sécurité des apps sous iOS et iPadOS

Aperçu de la sécurité des apps sous iOS et iPadOS

Contrairement aux autres plateformes mobiles, iOS et iPadOS n'autorisent pas les utilisateurs à installer des apps non signées potentiellement malveillantes à partir de sites Web ni à exécuter des apps non fiables. Lors de l'exécution, la signature du code vérifie les pages mémoire de tous les exécutables au fil de leur chargement pour contribuer à garantir qu'une app n'a pas été modifiée depuis son installation ou sa dernière mise à jour.

Après avoir vérifié qu'une app provient d'une source approuvée, iOS et iPadOS appliquent des mesures de sécurité destinées à l'empêcher de compromettre les autres apps ou le reste du système.

Signature du code sous iOS et iPadOS

Signature obligatoire du code

Après son démarrage, le noyau iOS ou iPadOS contrôle les apps et les processus utilisateur autorisés à s'exécuter. Pour aider à garantir que toutes les apps proviennent d'une source connue et approuvée et qu'elles n'ont pas été altérées, iOS et iPadOS exigent que l'ensemble du code exécutable soit signé à l'aide d'un certificat émis par Apple. Les apps fournies avec l'appareil, comme Mail et Safari, sont signées par Apple. Les apps tierces doivent également être validées et signées à l'aide d'un certificat émis par Apple. La signature obligatoire du code étend le concept de chaîne de confiance du système d'exploitation aux apps et contribue à empêcher les apps tierces de charger du code non signé ou d'utiliser du code susceptible de se modifier de façon autonome.

Signature des apps par les développeurs

Les développeurs peuvent signer leurs apps au moyen de la validation des certificats (par l'entremise du programme Apple pour les développeurs). Ils peuvent également intégrer un cadre d'application dans leurs apps et faire valider le code au moyen d'un certificat émis par Apple (par l'entremise d'une chaîne d'identifiant d'équipe).

- *Validation des certificats :* Pour développer des apps et les installer sur des appareils iOS ou iPadOS, les développeurs doivent s'inscrire auprès d'Apple et adhérer au programme Apple pour les développeurs. Apple vérifie l'identité réelle de chaque développeur, qu'il s'agisse d'une personne ou d'une entreprise, avant de lui remettre un certificat. Ce certificat permet aux développeurs de signer des apps et de les soumettre à l'App Store en vue de leur distribution. Ce processus garantit que toutes les apps de l'App Store ont été soumises par une personne ou une organisation identifiable, ce qui a pour effet de freiner la création d'apps malveillantes. Chaque app a également été vérifiée par Apple afin de contribuer à garantir qu'elle fonctionne conformément à la description fournie et qu'elle ne présente aucun bogue évident ni problème connu. En plus des technologies mentionnées précédemment, ce processus de sélection favorise la confiance des utilisateurs par rapport à la qualité des apps qu'ils achètent.
- *Validation de la signature du code :* iOS et iPadOS permettent aux développeurs d'incorporer des cadres d'application dans leurs apps; ceux-ci peuvent être utilisés par l'app elle-même ou par des extensions intégrées à celle-ci. Pour empêcher le système et les autres apps de charger du code tiers dans leur espace d'adressage, le système procède à une validation de la signature du code de toutes les bibliothèques dynamiques auxquelles un processus se lie lors de son lancement. Cette vérification est réalisée au moyen de l'identifiant d'équipe issu d'un certificat délivré par Apple. Un identifiant d'équipe est une chaîne alphanumérique comportant 10 caractères (par exemple 1A2B3C4D5F). Un programme peut s'associer à n'importe quelle bibliothèque fournie avec le système ou à n'importe quelle bibliothèque comportant dans la signature de son code le même identifiant d'équipe que l'exécutable principal. Comme les exécutables préinstallés sur le système ne possèdent pas d'identifiant d'équipe, ils ne peuvent s'associer qu'aux bibliothèques fournies avec le système.

Vérification des apps d'entreprise

Les entreprises ont également la possibilité de développer des apps réservées à un usage interne et de les distribuer à leurs employés. Les entreprises et les organisations peuvent déposer une candidature au programme Apple pour développeurs en entreprise (ADEP) avec un numéro D-U-N-S. Apple accepte les candidats après vérification de leur identité et de leur admissibilité. Une fois qu'une organisation est membre de l'ADEP, elle peut s'inscrire pour obtenir un profil d'approvisionnement permettant d'exécuter des apps internes sur des appareils autorisés.

Les utilisateurs doivent installer le profil d'approvisionnement pour pouvoir exécuter les apps internes. Cela contribue à garantir que seuls les utilisateurs concernés peuvent charger les apps sur leurs appareils iOS et iPadOS. Les apps installées à l'aide de la solution de gestion des appareils mobiles (GAM) sont considérées implicitement comme fiables, car la relation entre l'entreprise et l'appareil est déjà établie. Autrement, les utilisateurs doivent approuver le profil d'approvisionnement de l'app dans Réglages. Les entreprises peuvent empêcher les utilisateurs d'approuver des apps issues de développeurs inconnus. Au premier lancement d'une app d'entreprise quelconque, l'appareil doit recevoir la confirmation d'Apple que l'app est autorisée à s'exécuter.

Sécurité des processus d'exécution sous iOS et iPadOS

Mise en bac à sable

Toutes les apps tierces sont mises en bac à sable afin qu'elles ne puissent pas accéder aux fichiers stockés par les autres apps ni apporter de modifications à l'appareil. Cette façon de faire vise à empêcher les apps de collecter ou de modifier les informations stockées par les autres apps. Chaque app se voit attribuer de façon aléatoire un répertoire de départ unique pour ses fichiers lors de son installation. Si une app tierce doit accéder à des informations autres que les siennes, elle ne peut le faire qu'en utilisant les services explicitement fournis par iOS et iPadOS.

Les fichiers et ressources système sont également protégés des apps des utilisateurs. La plupart des fichiers et ressources système d'iOS et d'iPadOS s'exécutent en tant qu'utilisateur non privilégié « mobile », comme toutes les apps tierces. L'ensemble de la partition du système d'exploitation est monté en lecture seule. Les outils qui ne sont pas indispensables, comme les services de connexion à distance, ne sont pas inclus dans le logiciel système, et les API ne permettent pas aux apps d'augmenter leurs propres privilèges afin de modifier les autres apps ou iOS et iPadOS.

Utilisation des autorisations

L'accès des apps tierces aux renseignements de l'utilisateur et à certaines fonctionnalités comme iCloud et les capacités d'extension est contrôlé au moyen d'autorisations déclarées. Les autorisations sont des paires clé-valeur qui sont connectées à une app et qui permettent l'authentification en dehors des facteurs d'exécution, comme l'identifiant d'utilisateur UNIX. Les autorisations étant signées numériquement, elles ne peuvent pas être modifiées. Les autorisations sont couramment utilisées par les apps et les démons système pour réaliser certaines opérations privilégiées pour lesquelles le processus devrait normalement s'exécuter en tant que racine. Cela réduit grandement la possibilité qu'une app ou un démon système compromis accède à des privilèges supérieurs.

En outre, les apps ne peuvent réaliser un traitement en arrière-plan qu'au moyen d'API fournies par le système. Cela leur permet de continuer à s'exécuter sans affecter les performances ni réduire de façon importante l'autonomie de la batterie.

Distribution aléatoire de l'espace d'adressage (ASLR)

La distribution aléatoire de l'espace d'adressage (ASLR, Address Space Layout Randomization) contribue à empêcher l'exploitation des bogues de corruption de la mémoire. Les apps intégrées utilisent l'ASLR pour contribuer à la distribution aléatoire de toutes les zones de la mémoire au lancement. L'organisation aléatoire des adresses mémoire du code exécutable, des bibliothèques système et des structures de programmation associées réduit la probabilité de nombreux exploits. Par exemple, une attaque de type return-to-libc tente d'amener un appareil à exécuter un programme malveillant en manipulant les adresses mémoire des bibliothèques système et de la pile. L'organisation aléatoire de celles-ci rend l'attaque plus difficile à exécuter, en particulier sur plusieurs appareils. Xcode et l'environnement de développement d'iOS ou iPadOS compilent automatiquement les programmes tiers avec la prise en charge de l'ASLR activée.

Fonctionnalité Execute Never

Une protection supplémentaire est apportée par iOS et iPadOS à l'aide du bit XN (Execute Never) du processeur ARM, qui permet de marquer des pages mémoire comme non exécutables. Les pages mémoire marquées à la fois comme accessibles en écriture et exécutables ne peuvent être utilisées par les apps que dans des conditions étroitement contrôlées : le noyau vérifie la présence de l'autorisation de signature de code dynamique exclusive à Apple. Même dans ce cas, un seul appel `mmap` est autorisé pour demander une page exécutable et accessible en écriture, laquelle se voit assigner une adresse de façon aléatoire. Safari utilise cette fonctionnalité pour son compilateur JIT JavaScript.

Prise en charge des extensions sous iOS, iPadOS et macOS

iOS, iPadOS et macOS permettent aux apps d'étendre les fonctionnalités d'autres apps au moyen d'extensions. Incorporées dans une app, les extensions sont des exécutables binaires signés ayant une fonction spéciale. Au cours de l'installation, le système détecte automatiquement les extensions et les met à la disposition des autres apps à l'aide d'un système de mise en correspondance.

Points d'extension

Une zone système prenant en charge les extensions est appelée *point d'extension*. Chaque point d'extension fournit des API et applique des règles pour cette zone. Le système détermine quelles extensions sont disponibles d'après des règles de mise en correspondance propres au point d'extension. Le système lance automatiquement les processus d'extension lorsque cela est nécessaire et gère leur durée de vie. Des déclarations d'autorisation peuvent être utilisées pour limiter la disponibilité des extensions à des apps système précises. Par exemple, un widget d'affichage Aujourd'hui n'apparaît que dans le Centre de notifications, et une extension de partage n'est disponible que dans la sous-fenêtre Partage. Les points d'extension sont, par exemple, les widgets Aujourd'hui; Partager; Actions; Édition photo; Fournisseur de fichier; et Clavier personnalisé.

Communication des extensions

Les extensions s'exécutent dans leur propre espace d'adressage. La communication entre une extension et l'app à partir de laquelle elle a été activée se fait via des communications interprocessus assistées par le cadre d'application système. Les extensions n'ont pas accès aux fichiers ni aux espaces mémoire des autres extensions. Elles sont conçues pour être isolées les unes des autres, de l'app qui les contient et des apps qui les utilisent. Elles sont mises en bac à sable comme toute autre app tierce et possèdent un conteneur distinct de celui de l'app. Toutefois, elles partagent le même accès aux contrôles de confidentialité que l'app qui les contient. Ainsi, si un utilisateur accorde l'accès aux contacts à une app, cette autorisation est étendue aux extensions intégrées à celle-ci, mais pas aux extensions activées par celle-ci.

Utilisation des claviers personnalisés

Les claviers personnalisés sont un type spécial d'extensions dans la mesure où ils sont activés par l'utilisateur pour l'ensemble du système. Une fois activée, l'extension de clavier est utilisée pour toute saisie de texte, à l'exception des codes et de tout autre texte saisi dans une vue sécurisée. Pour limiter le transfert des données utilisateur, les claviers personnalisés s'exécutent par défaut dans un bac à sable très restrictif bloquant l'accès au réseau, aux services réalisant des opérations réseau pour le compte d'un processus et aux API qui permettraient à l'extension d'envoyer les données saisies. Les développeurs de claviers personnalisés peuvent demander à ce que leur extension bénéficie d'un accès libre, ce qui permet au système de l'exécuter dans le bac à sable par défaut après obtention du consentement de l'utilisateur.

Gestion des appareils mobiles (GAM) et extensions

Pour les appareils inscrits à une solution de gestion des appareils mobiles, les extensions de document et de clavier obéissent aux règles de gestion des autorisations d'ouverture (Managed Open In). Par exemple, la solution de GAM peut contribuer à empêcher les utilisateurs d'exporter un document d'une app gérée vers un fournisseur de documents non géré, ou d'utiliser un clavier non géré avec une app gérée. En outre, les développeurs d'apps peuvent empêcher l'utilisation d'extensions de clavier tierces avec leur app.

Protection des apps et groupes d'apps sous iOS et iPadOS

Adoption de la protection des données dans les apps

La trousse de développement logiciel (SDK) pour iOS et iPadOS offre un éventail complet d'API permettant aux développeurs tiers et internes d'adopter facilement la protection des données et d'assurer un niveau de protection maximal dans leurs apps. La protection des données est disponible pour les API de fichiers et de bases de données, notamment NSFileManager, CoreData, NSData et SQLite.

La base de données de l'app Mail (y compris les pièces jointes), les livres gérés, les signets Safari, les images de lancement d'app et les données de localisation sont également stockées par chiffrement avec des clés protégées par le code de l'utilisateur sur son appareil. Les apps Calendrier (à l'exception des pièces jointes), Contacts, Rappels, Notes, Messages et Photos utilisent le droit de protection des données « Protection complète jusqu'à la première authentification de l'utilisateur ».

Les apps installées par l'utilisateur qui n'optent pas pour une classe de protection des données déterminée reçoivent par défaut la classe « Protection complète jusqu'à la première authentification de l'utilisateur ».

Intégration à un groupe d'apps

Les apps et les extensions appartenant à un compte de développeur donné peuvent partager du contenu lorsqu'elles sont intégrées au même groupe d'apps. Il appartient au développeur de créer les groupes appropriés sur le portail Apple Developer et d'y inclure les apps et les extensions souhaitées. Une fois intégrées à un groupe d'apps, les apps ont accès aux éléments suivants :

- un conteneur sur volume partagé pour le stockage, qui reste sur l'appareil tant qu'au moins une app du groupe est installée;

- des préférences partagées;
- des éléments de trousseau partagés.

Le portail Apple Developer contribue à garantir que les identifiants de groupe (GID) d'apps sont uniques dans l'ensemble de l'écosystème d'apps.

Vérification des accessoires sous iOS et iPadOS

Le programme d'homologation Made for iPhone, iPad et iPod touch (MFi) permet aux fabricants d'accessoires approuvés d'accéder au protocole d'accessoires iPod (iAP) et aux composants matériels de prise en charge nécessaires.

Lorsqu'un accessoire MFi communique avec un appareil iOS ou iPadOS à l'aide d'un connecteur Lightning ou USB-C, ou par Bluetooth, l'appareil demande à l'accessoire de prouver qu'il a été autorisé par Apple en répondant avec un certificat fourni par Apple, qui est vérifié par l'appareil. L'appareil envoie ensuite un défi auquel l'accessoire doit répondre à l'aide d'une réponse signée. Ce processus est entièrement géré par un circuit intégré (CI) sur mesure qu'Apple fournit aux fabricants d'accessoires approuvés et se fait en toute transparence pour l'accessoire.

Les accessoires peuvent demander l'accès à différentes fonctionnalités et méthodes de transport, comme l'accès à des flux audio numériques sur le câble Lightning ou USB-C, ou à des informations de localisation fournies par Bluetooth. Un CI d'authentification est conçu pour garantir que seuls les accessoires approuvés se voient accorder l'accès complet à l'appareil. Si un accessoire ne prend pas en charge l'authentification, son accès est limité au flux audio analogique et à un sous-ensemble restreint de commandes de lecture audio série (UART).

AirPlay utilise également le CI d'authentification pour vérifier que les récepteurs ont été approuvés par Apple. Les flux audio AirPlay et vidéo CarPlay emploient le protocole MFi-SAP (Secure Association Protocol), qui chiffre les communications entre l'accessoire et l'appareil à l'aide du protocole AES-128 en mode basé sur un compteur (CTR). Des clés éphémères sont échangées à l'aide du protocole d'échange de clés ECDH (Curve25519) et signées à l'aide de la clé RSA 1 024 bits du CI d'authentification dans le cadre du protocole Station-to-Station (STS).

Sécurité des apps sous macOS

Aperçu de la sécurité des apps sous macOS

La sécurité des apps sous macOS consiste en un nombre de couches superposées, dont la première est l'option de n'exécuter que les apps signées et fiables provenant de l'App Store. De plus, macOS superpose les protections pour contribuer à prévenir la présence de logiciels malveillants connus dans les apps téléchargées à partir d'Internet. macOS propose des technologies pour détecter et supprimer les logiciels malveillants en plus d'offrir des protections supplémentaires conçues pour empêcher les apps non vérifiées d'accéder aux données des utilisateurs. Les services d'Apple, comme la notarisation et XProtect, ainsi que les mises à jour de l'outil de suppression de logiciels malveillants sont conçus pour empêcher l'installation de logiciels malveillants et, lorsque c'est nécessaire, pour fournir un processus de détection et de réponse rapide et efficace destiné à bloquer et à supprimer tout logiciel malveillant susceptible d'avoir évité dans un premier temps la détection. Enfin, les utilisateurs de macOS peuvent utiliser le modèle de sécurité qui leur convient le mieux, y compris l'exécution de code non signé et non fiable.

Signature du code des apps sous macOS

Toutes les apps de l'App Store sont signées par Apple. Cette signature vise à garantir qu'elles n'ont pas été altérées. Apple signe également les apps préinstallées sur ses appareils.

Sous macOS 10.15, toutes les apps qui ne proviennent pas de l'App Store doivent être signées par le développeur à l'aide d'un certificat d'identification délivré par Apple (associé à une clé privée) et notarisées par Apple, afin que la fonctionnalité Gatekeeper, si elle est configurée par défaut, autorise leur exécution. Les apps maison doivent également être signées avec un certificat de développeur délivré par Apple pour que les utilisateurs puissent en valider l'intégrité.

Sous macOS, la notarisation et la signature de code fonctionnent séparément et peuvent être effectuées par différents acteurs et à des fins différentes. La signature de code est effectuée par le développeur au moyen du certificat d'identification délivré par Apple, et la vérification de cette signature prouve à l'utilisateur que le logiciel d'un développeur n'a pas été altéré depuis sa conception et sa signature. La notarisation peut être effectuée par quiconque participe à la chaîne de distribution du logiciel et prouve qu'Apple a reçu une copie du code pour confirmer l'absence de tout logiciel malveillant. Un ticket de notarisation, stocké sur les serveurs Apple, peut être facultativement joint à l'app (par n'importe qui) sans invalider la signature du développeur.

Les contrôles d'accès obligatoires requièrent la signature du code pour activer les déclarations d'autorisation protégées par le système. Par exemple, les apps qui demandent à traverser le coupe-feu doivent détenir un code signé assorti de l'autorisation appropriée émanant des contrôles d'accès obligatoires.

Gatekeeper et protection à l’exécution sous macOS

Gatekeeper

macOS comprend la technologie Gatekeeper, qui, par défaut, est conçue pour ne laisser s’exécuter sur le Mac d’un utilisateur que les logiciels vérifiés. Quand un utilisateur télécharge et ouvre une app, un module ou un paquet d’installation qui ne provient pas de l’App Store, Gatekeeper vérifie que le logiciel est assorti d’un certificat d’identification du développeur valide et qu’il est notarisé par Apple comme étant exempt de contenu malveillant et d’altérations. Gatekeeper requiert également l’approbation de l’utilisateur avant la première ouverture d’un logiciel téléchargé afin de vérifier que l’utilisateur n’a pas été amené à lancer un code exécutable qu’il croyait être simplement un fichier de données.

Par défaut, Gatekeeper contribue à vérifier que tous les logiciels téléchargés ont été signés par l’App Store ou un développeur certifié, puis notarisés par Apple. Ensemble, la vérification sur l’App Store et le processus de notarisation visent à garantir que les apps ne contiennent aucun logiciel malveillant connu. Par conséquent, *tous les logiciels sous macOS sont analysés par défaut pour déceler la présence de contenu malveillant lors de leur première ouverture, peu importe comment ils ont été installés sur le Mac.*

Les utilisateurs et les organisations ont la possibilité d’autoriser uniquement les logiciels installés à partir de l’App Store. Sinon, les utilisateurs peuvent outrepasser les politiques de Gatekeeper pour ouvrir n’importe quel logiciel, à moins de restrictions imposées par une solution de gestion des appareils mobiles (GAM). Les organisations peuvent utiliser la GAM pour configurer les réglages de Gatekeeper, y compris l’autorisation de logiciels signés par d’autres identités. Il est également possible de complètement désactiver Gatekeeper, au besoin.

Gatekeeper prévient aussi la distribution de modules malveillants avec des apps bénignes. Dans une telle situation, l’utilisation de l’app déclenche le chargement d’un module malveillant à l’insu de l’utilisateur. Lorsqu’il le faut, Gatekeeper ouvre les apps depuis des emplacements aléatoires en lecture seule, ce qui vise à empêcher le chargement automatique de modules distribués avec l’app.

Protection à l’exécution

Les fichiers et ressources système et le noyau sont isolés de l’espace d’exécution des apps de l’utilisateur. Les apps provenant de l’App Store sont mises en bac à sable pour qu’elles ne puissent pas accéder aux données stockées par d’autres apps. Si une app provenant de l’App Store doit accéder aux données d’une autre app, elle ne peut le faire qu’en recourant aux API et aux services fournis par macOS.

Protection contre les logiciels malveillants sous macOS

Apple exécute un processus qui exploite les renseignements sur les menaces pour identifier et bloquer rapidement les logiciels malveillants. Les défenses contre les logiciels malveillants sont organisées en trois couches :

1. *Empêcher le lancement ou l’exécution des logiciels malveillants :* App Store ou Gatekeeper et la notarisation

2. *Bloquer l’exécution des logiciels malveillants sur les systèmes clients :* Gatekeeper, la notarisation et XProtect

3. *Remédier à l'infection causée par l'exécution de tout logiciel malveillant :* l'outil de suppression de logiciels malveillants (MRT)

La première couche de défense est conçue pour contenir la distribution de logiciels malveillants et pour empêcher ces derniers de s'exécuter ne serait-ce qu'une fois. C'est le rôle de l'*App Store* et de *Gatekeeper* combinés à la *notarisation*.

La couche de défense suivante a pour mission d'aider à identifier et à bloquer rapidement tout logiciel malveillant qui parvient à s'introduire sur un Mac, et ce, dans le but d'arrêter sa propagation et de réhabiliter les systèmes déjà touchés sur le Mac. En plus de Gatekeeper et de la notarisation, cette couche de défense compte aussi sur *XProtect*.

Enfin, le *MRT* agit pour réparer les méfaits de tout logiciel malveillant qui a réussi malgré tout à s'exécuter.

Ces protections s'allient pour soutenir les bonnes pratiques de sécurité contre les virus et les logiciels malveillants. Il existe des mesures de protection supplémentaires, particulièrement sur les Mac dotés d'une puce Apple, pour limiter les dommages que les logiciels malveillants sont en mesure de causer lorsqu'ils parviennent à s'exécuter. Consultez la section Protections contre l'accès des apps aux données utilisateur pour découvrir comment macOS peut contribuer à protéger les données utilisateur des logiciels malveillants, et la section Intégrité du système d'exploitation pour découvrir comment macOS peut limiter les actions qu'un logiciel malveillant peut entreprendre sur le système.

Notarisation

La *notarisation* est un service d'analyse de logiciels malveillants fourni par Apple. Les développeurs qui souhaitent distribuer des apps pour macOS en dehors de l'App Store soumettent leurs apps à des fins d'analyse dans le cadre du processus de distribution. Apple analyse ces logiciels afin d'identifier tout logiciel malveillant connu, puis émet un ticket de notarisation si aucun logiciel malveillant n'a été détecté. Les développeurs ajoutent généralement ce ticket à leur app pour que Gatekeeper puisse vérifier et lancer l'app, même lorsque l'ordinateur est hors ligne.

Apple peut aussi émettre un ticket de révocation aux apps connues pour être malveillantes, et ce, même si elles ont été précédemment notarisées. macOS consulte régulièrement les nouveaux tickets de révocation pour que Gatekeeper puisse disposer des informations les plus récentes et bloquer le lancement de tels fichiers. Ce processus peut bloquer très rapidement les apps malveillantes parce que les mises à jour ont lieu en arrière-plan beaucoup plus fréquemment que celles qui envoient les nouvelles signatures XProtect en arrière-plan. Par ailleurs, cette protection peut être appliquée tant aux apps qui ont déjà été notarisées qu'à celles qui ne l'ont jamais été.

XProtect

macOS comporte une technologie antivirus appelée *XProtect* pour détecter les logiciels malveillants sur la base de leur signature. Le système utilise des signatures YARA, un outil qu'Apple met à jour régulièrement qui sert à détecter les logiciels malveillants sur la base de leur signature. Apple surveille l'apparition de nouveaux logiciels malveillants et actualise automatiquement la liste de signatures, indépendamment des mises à jour du système, pour empêcher un Mac d'être infecté. XProtect détecte les logiciels malveillants connus et bloque leur exécution. Sous macOS 10.15 et les versions ultérieures, XProtect vérifie la présence de contenu malveillant connu dès :

- qu’une app est lancée pour la première fois;
- qu’une app a été modifiée (dans le système de fichiers);
- que les signatures XProtect sont mises à jour.

S’il détecte un logiciel malveillant connu, XProtect bloque le programme, puis l’utilisateur reçoit une notification et peut choisir de le placer dans la corbeille.

Remarque : La notarisation est efficace dans le cas des fichiers (ou des hachages de fichiers) connus et peut être utilisée avec les apps qui ont déjà été lancées. Les règles de XProtect qui reposent sur les signatures sont plus génériques que le hachage d’un fichier donné. XProtect est donc en mesure de détecter des variantes qu’Apple n’a pas distinguées. Le cycle de mise à jour de XProtect est plus lent que la notarisation. Par ailleurs, XProtect n’analyse les apps que lors de leur premier lancement ou lorsqu’elles subissent une modification.

Outil de suppression de logiciels malveillants

macOS comprend des technologies pour remédier à l’infection d’un Mac par un programme malveillant. L’*outil de suppression de logiciels malveillants (MRT)* est un moteur de macOS qui remédie aux infections en fonction des mises à jour automatiquement transmises par Apple (dans le cadre des mises à jour automatiques des fichiers de données système et de la sécurité). Le MRT supprime les programmes malveillants dès la réception d’informations à jour, et continue de vérifier la présence d’infections pendant le redémarrage et la connexion. Le MRT ne redémarre pas le Mac automatiquement.

Mises à jour de sécurité automatiques

Apple publie automatiquement des mises à jour pour XProtect et le MRT en fonction des derniers renseignements sur les menaces. Par défaut, macOS recherche ces mises à jour quotidiennement. Les mises à jour de notarisation sont distribuées par l’entremise de la synchronisation de CloudKit et sont bien plus fréquentes.

Procédure d’intervention

Lorsqu’un nouveau logiciel malveillant est découvert, plusieurs opérations peuvent être effectuées :

- Tous les certificats d’identification du développeur associés sont révoqués.
- Les tickets de révocation de notarisation sont émis pour tous les fichiers (apps et fichiers associés).
- Les signatures XProtect sont développées et distribuées.
- Les signatures MRT sont développées et distribuées.
- Ces signatures sont également appliquées de façon rétroactive aux logiciels précédemment notarisés et toute nouvelle détection peut entraîner une ou plusieurs des actions précédentes.

En définitive, la détection d’un logiciel malveillant déclenche une série d’opérations au cours des prochaines secondes, heures et journées pour offrir la meilleure protection possible aux utilisateurs de Mac.

Contrôle de l’accès des apps aux fichiers sous macOS

Chez Apple, nous croyons que les utilisateurs devraient profiter d’une transparence et d’un contrôle complets sur ce que les apps font avec leurs données et pouvoir y consentir. Sous macOS 10.15, ce modèle est appliqué par le système pour contribuer à garantir que toutes les apps doivent obtenir le consentement de l’utilisateur avant d’accéder aux fichiers dans Documents, Téléchargements, Bureau et iCloud Drive ainsi que sur les volumes réseau. Sous macOS 10.13 et les versions ultérieures, les apps qui demandent l’accès à l’intégralité du dispositif de stockage doivent être explicitement ajoutées dans les Préférences Système. De plus, les fonctionnalités d’accessibilité et d’automatisation nécessitent l’autorisation de l’utilisateur pour contribuer à garantir qu’elles ne contournent pas d’autres protections. Selon la politique d’accès, les utilisateurs peuvent être invités ou forcés à modifier les réglages dans Préférences Système > Sécurité et confidentialité > Confidentialité.

Élément	L’utilisateur est invité par l’app	L’utilisateur doit modifier les réglages de confidentialité du système
Accessibilité		✅
Accès à l’intégralité du stockage interne		✅
Fichiers et dossiers *Remarque :* Comprend : Bureau, Documents, Téléchargements, les volumes réseau et les volumes amovibles	✅	
Automatisation (événements Apple)	✅	

Les éléments dans la corbeille de l’utilisateur sont protégés contre les apps qui ont un accès complet au disque. L’utilisateur ne sera pas invité à autoriser ou non l’accès. Les fichiers contenus dans la corbeille doivent être déplacés vers un autre emplacement si l’utilisateur souhaite que les apps puissent y accéder.

Quand FileVault est activé, le Mac demande à l’utilisateur de s’authentifier avant de poursuivre le démarrage et de donner accès aux modes de démarrage spécialisés. Si l’utilisateur ne fournit pas les bonnes informations d’identification ou la clé de secours, le volume demeure chiffré et protégé contre les accès non autorisés, même si le dispositif de stockage est retiré du Mac et branché à un autre ordinateur.

Pour protéger les données en entreprise, les équipes des TI doivent définir une politique claire pour la configuration de FileVault et l’imposer par l’intermédiaire de la solution de gestion des appareils mobiles (GAM). Les organisations disposent de plusieurs options pour la gestion des volumes chiffrés, comme les clés de secours institutionnelles, les clés de secours personnelles (qui peuvent être enregistrées dans la solution de GAM pour l’autorité de séquestre), ou une combinaison des deux. La rotation de clés peut elle aussi faire l’objet d’une politique de GAM.

Fonctionnalités de sécurité dans l’app Notes

Notes sécurisées

L’app Notes comprend une fonctionnalité de notes sécurisées permettant aux utilisateurs de protéger le contenu de certaines notes. Les notes sécurisées sont chiffrées de bout en bout à l’aide d’une phrase secrète fournie par l’utilisateur et requise pour afficher les notes sur les appareils iOS, iPadOS et macOS, ainsi que sur le site Web d’iCloud. Une phrase secrète peut être définie pour chaque compte iCloud (y compris les comptes d’appareil « Sur mon »).

Lorsqu’un utilisateur sécurise une note, une clé sur 16 octets est calculée d’après la phrase secrète de l’utilisateur avec les algorithmes PBKDF2 et SHA256. La note et toutes ses pièces jointes sont chiffrées à l’aide de l’algorithme AES en mode Galois/Counter Mode (AES-GCM). De nouveaux enregistrements sont créés dans Core Data et CloudKit pour stocker la note, les pièces jointes, l’étiquette et le vecteur d’initialisation chiffrés. Après la création des nouveaux enregistrements, les données d’origine non chiffrées sont supprimées. Les pièces jointes qui prennent en charge le chiffrement comprennent les images, les dessins, les tableaux, les plans et les sites Web. Les notes contenant d’autres types de pièces jointes ne peuvent pas être chiffrées, et ces pièces jointes ne peuvent être ajoutées aux notes sécurisées.

Pour afficher une note sécurisée, l’utilisateur doit saisir la phrase secrète ou s’identifier avec Touch ID ou Face ID. Après l’authentification de l’utilisateur, que ce soit pour afficher ou pour créer une note sécurisée, Notes ouvre une session sécurisée. Dans cette session, l’utilisateur peut afficher ou sécuriser d’autres notes sans authentification supplémentaire. Cependant, la session sécurisée ne s’applique qu’aux notes protégées à l’aide de la phrase secrète fournie. L’utilisateur doit quand même s’identifier pour les notes protégées par une autre phrase secrète. La session sécurisée prend fin lorsque :

- l’utilisateur touche le bouton Verrouiller dans Notes;
- l’app Notes se trouve en arrière-plan pendant plus de trois minutes (huit minutes sous macOS);
- l’appareil iOS ou iPadOS se verrouille.

Pour modifier la phrase secrète d’une note sécurisée, l’utilisateur doit saisir la phrase secrète actuelle, puisque Touch ID et Face ID ne sont pas disponibles lors de cette opération. Après que l’utilisateur a choisi une nouvelle phrase secrète, l’app Notes enveloppe de nouveau les clés de toutes les notes du même compte qui avaient été chiffrées avec l’ancienne phrase secrète.

Si l’utilisateur saisit une mauvaise phrase trois fois de suite, Notes affiche un indice si l’utilisateur en a fourni un lors de la configuration. Si l’utilisateur ne se souvient pas de sa phrase secrète, il peut la réinitialiser dans les réglages de Notes. Cette fonctionnalité lui permet de créer de nouvelles notes sécurisées à l’aide d’une nouvelle phrase secrète, mais l’utilisateur ne pourra consulter les notes sécurisées avec l’ancienne phrase secrète. Il est toutefois possible d’afficher les notes précédemment sécurisées si l’utilisateur se souvient de l’ancienne phrase secrète. La phrase secrète du compte iCloud de l’utilisateur est requise pour réinitialiser la phrase secrète dans Notes.

Notes partagées

Les notes qui ne sont pas chiffrées de bout en bout à l'aide d'une phrase secrète peuvent être partagées avec d'autres utilisateurs. Les notes partagées utilisent encore le type de données chiffrées CloudKit pour tout texte ou toute pièce jointe que l'utilisateur ajoute à une note. Le contenu est toujours chiffré avec une clé chiffrée dans CKRecord. Les métadonnées, comme les dates de création et de modification, ne sont pas chiffrées. CloudKit gère le processus qui régit les participants autorisés ou non à chiffrer ou à déchiffrer les données des notes partagées.

Fonctionnalités de sécurité dans l'app Raccourcis

Dans l'app Raccourcis, les raccourcis sont facultativement synchronisés sur tous les appareils Apple à l'aide d'iCloud. Les raccourcis peuvent également être partagés avec d'autres utilisateurs par iCloud. Les raccourcis sont stockés localement dans un format chiffré.

Les raccourcis personnalisés sont polyvalents, comme des scripts ou des programmes. Quand il télécharge un raccourci par Internet, l'utilisateur est avisé que le raccourci n'a pas encore été examiné par Apple et a l'occasion d'inspecter le raccourci. À titre de protection contre les raccourcis malveillants, des définitions de logiciels malveillants à jour sont téléchargées pour identifier les raccourcis malveillants à l'exécution.

Les raccourcis personnalisés peuvent également exécuter un code JavaScript défini par l'utilisateur sur les sites Web dans Safari lorsqu'ils sont appelés à partir de la fiche de partage. À titre de protection contre un code JavaScript malveillant qui, par exemple, amènerait l'utilisateur à exécuter un script sur un site de médias sociaux qui recueille ses données, le code JavaScript est validé en fonction des définitions de logiciels malveillants susmentionnées. La première fois qu'il exécute du code JavaScript sur un domaine, l'utilisateur est invité à autoriser les raccourcis contenant du JavaScript à s'exécuter sur la page Web actuelle pour ce domaine.

Sécurité des services

Aperçu de la sécurité des services

Apple a mis en place un vaste éventail de services permettant aux utilisateurs d'en faire encore plus avec leurs appareils. Tous offrent de puissantes fonctionnalités – que ce soit pour le stockage dans le nuage, la synchronisation, le stockage de mots de passe, l'authentification, les paiements, l'envoi de messages, les communications et plus encore – tout en veillant à la confidentialité et à la sécurité des données des usagers.

Ces services, qui comprennent iCloud, Connexion avec Apple, Apple Pay, iMessage, FaceTime, Localiser, Continuité et le clavardage commercial, peuvent nécessiter un identifiant Apple ou un identifiant Apple géré. Il est possible qu'un identifiant Apple géré ne puisse pas être utilisé pour certains services, par exemple Apple Pay.

Remarque : Certains contenus et services Apple pourraient ne pas être offerts dans tous les pays ou toutes les régions.

Identifiant Apple et identifiant Apple géré

Aperçu de la sécurité de l'identifiant Apple

Aperçu

L'identifiant Apple est un compte qui permet de se connecter à des services Apple, tels qu'iCloud, iMessage, FaceTime, l'iTunes Store, l'App Store, l'app Apple TV, Apple Books et plus encore. Il est essentiel que chaque utilisateur protège son identifiant Apple afin de contribuer à éviter tout accès non autorisé à ses comptes. Pour y arriver, les identifiants Apple requièrent des mots de passe robustes qui :

- comptent au moins huit caractères;
- contiennent des lettres et des chiffres;
- ne contiennent pas plus de trois caractères identiques consécutifs;
- ne sont pas couramment utilisés.

Les utilisateurs sont encouragés à aller au-delà de ces recommandations en ajoutant des caractères et des signes de ponctuation pour renforcer leurs mots de passe.

Apple avertit les utilisateurs par courriel ou notification Push lorsque des modifications importantes sont apportées à leur compte, par exemple si le mot de passe ou les données de facturation sont modifiés, ou encore si l'identifiant Apple est utilisé pour se connecter à un nouvel appareil. Les utilisateurs sont invités à changer le mot de passe de leur identifiant Apple dès qu'ils remarquent quoi que ce soit d'inhabituel.

En outre, Apple adopte de multiples politiques et procédures conçues pour protéger les comptes utilisateur. Parmi ces dispositions, on retrouve la limitation du nombre de tentatives de connexion et de réinitialisation du mot de passe, la surveillance active des fraudes pour aider à repérer les attaques dès qu'elles se produisent, ainsi que l'examen périodique des règles pour aider Apple à s'adapter à toute nouvelle information susceptible de compromettre la sécurité des utilisateurs.

Remarque : La règle de mot de passe de l'identifiant Apple géré est définie par l'administrateur dans Apple School Manager ou Apple Business Manager.

Authentification à deux facteurs

Pour aider les utilisateurs à sécuriser davantage leur compte, Apple propose l'*authentification à deux facteurs*, une couche de sécurité supplémentaire pour les identifiants Apple. Elle est conçue pour que seul le propriétaire du compte puisse y accéder, même si quelqu'un d'autre connaît le mot de passe. Avec l'authentification à deux facteurs, le compte d'un utilisateur est accessible uniquement sur les appareils de confiance, tels que son iPhone, son iPad, son iPod touch ou son Mac, ou d'autres appareils après leur vérification depuis un de ces appareils approuvés ou un numéro de téléphone de confiance. Pour une première connexion sur un nouvel appareil, deux informations sont requises : le mot de passe de l'identifiant Apple et un code de vérification à six chiffres affiché sur les appareils approuvés par l'utilisateur ou envoyé à un numéro de téléphone de confiance. En saisissant le code, l'utilisateur confirme qu'il fait confiance au nouvel appareil et que celui-ci peut être utilisé pour se connecter. Puisqu'un simple mot de passe n'est plus suffisant pour accéder au compte d'un utilisateur, l'authentification à deux facteurs améliore la sécurité de l'identifiant Apple de l'utilisateur et de toutes les informations personnelles qu'il stocke auprès d'Apple. Cette technique est directement intégrée à iOS, à iPadOS, à macOS, à tvOS, à watchOS et aux systèmes d'authentification employés par les sites Web d'Apple.

Lorsqu'un utilisateur se connecte à un site Web d'Apple sur un navigateur Web, une demande de deuxième facteur est envoyée à tous les appareils approuvés associés à son compte iCloud pour approuver la session Web. Si l'utilisateur se connecte à un site Web d'Apple à partir d'un navigateur sur un appareil approuvé, le code de vérification s'affiche localement sur cet appareil. Lorsque l'utilisateur entre le code sur cet appareil, la session Web est approuvée.

Récupération de compte

En cas d'oubli du mot de passe d'un identifiant Apple, l'utilisateur peut le réinitialiser sur un appareil de confiance. Si aucun appareil approuvé n'est disponible et que le mot de passe est connu, l'utilisateur peut utiliser un numéro de téléphone de confiance pour procéder à l'authentification par messagerie texte (SMS). De plus, pour permettre une récupération immédiate d'un identifiant Apple, un ancien code peut être utilisé pour procéder à la réinitialisation conjointement avec un SMS. Si ces options sont impossibles, l'utilisateur devra suivre le processus de récupération de compte. Pour en savoir plus, consultez l'article de l'assistance Apple Comment utiliser la récupération de compte lorsque vous ne pouvez pas réinitialiser le mot de passe associé à votre identifiant Apple.

Identifiant Apple géré

Les identifiants Apple gérés fonctionnent comme les identifiants Apple, mais sont détenus et contrôlés par une entreprise ou un établissement d'enseignement. Les organisations peuvent réinitialiser les mots de passe, limiter les achats et les communications, par exemple celles effectuées au moyen de FaceTime et de Messages, et configurer des autorisations qui reposent sur des rôles pour les membres du personnel, les professeurs et les élèves.

Pour les identifiants Apple gérés, certains services sont désactivés (par exemple Apple Pay, le trousseau iCloud, HomeKit et Localiser).

Inspection des identifiants Apple gérés

Les identifiants Apple gérés prennent également en charge l'*inspection*, ce qui permet aux organisations de se conformer aux lois et aux réglementations en matière de confidentialité. Un administrateur Apple School Manager, un gestionnaire ou un enseignant peut inspecter un identifiant Apple géré donné.

Les inspecteurs sont en mesure de contrôler uniquement les comptes qui dépendent d'eux dans la hiérarchie de l'organisation. Par exemple, les enseignants peuvent surveiller les élèves, les gestionnaires peuvent surveiller les enseignants et les élèves, et les administrateurs peuvent effectuer l'inspection des gestionnaires, des enseignants et des élèves.

Lorsque des informations d'authentification associées à la réalisation d'une inspection sont demandées via Apple School Manager, un compte spécial est créé. Ce compte a uniquement accès à l'identifiant Apple géré pour lequel l'inspection est demandée. L'inspecteur peut ensuite lire et modifier le contenu de l'utilisateur stocké sur iCloud ou dans les apps qui utilisent CloudKit. Chaque demande d'accès relative à une inspection est consignée dans Apple School Manager. Le journal indique qui est l'inspecteur, l'identifiant Apple géré pour lequel l'inspecteur a demandé l'accès, l'heure de la demande et si l'inspection a été réalisée.

Identifiants Apple gérés et appareils personnels

Les identifiants Apple gérés peuvent également être utilisés avec des appareils iOS, des appareils iPadOS ou des ordinateurs Mac personnels. Les élèves se connectent à iCloud avec l'identifiant Apple géré attribué par l'établissement et un autre mot de passe à usage personnel faisant office de deuxième facteur lors du processus d'authentification à deux facteurs pour l'identifiant Apple. Lorsque les élèves utilisent un identifiant Apple géré sur un appareil personnel, le trousseau iCloud est indisponible, et l'établissement peut restreindre d'autres fonctionnalités comme FaceTime ou Messages. Tout document iCloud créé par des élèves lorsqu'ils sont connectés est susceptible de faire l'objet d'une inspection comme il a été décrit précédemment dans la présente section.

iCloud

Aperçu de la sécurité iCloud

iCloud est utilisé pour stocker les contacts, les calendriers, les photos, les documents et d'autres données d'un utilisateur, et tenir automatiquement ces informations à jour sur tous les appareils de ce dernier. iCloud peut également être utilisé par des apps tierces pour stocker et synchroniser des documents ainsi que des valeurs de clé de données d'app définies par le développeur. Chaque utilisateur configure son espace iCloud en se connectant au moyen d'un identifiant Apple et en choisissant les services qu'il souhaite utiliser. Certaines fonctionnalités iCloud, iCloud Drive et la sauvegarde iCloud peuvent être désactivés par les administrateurs des TI à l'aide des profils de configuration de la gestion des appareils mobiles (GAM). Le service ne tient pas compte du contenu stocké et traite le contenu de tous les fichiers de la même manière, comme s'il s'agissait de simples regroupements d'octets.

Chaque fichier est divisé en blocs et chiffré par iCloud à l'aide de l'algorithme AES128 et d'une clé dérivée du contenu de chaque partie; les clés utilisent l'algorithme SHA256. Les clés et les métadonnées du fichier sont stockées par Apple dans le compte iCloud de l'utilisateur. Les blocs chiffrés du fichier sont stockés, sans les informations d'identification de l'utilisateur ni les clés, par l'entremise de services de stockage d'Apple et de tiers, comme Amazon Web Services ou Google Cloud. Ces partenaires ne possèdent pas les clés pour déchiffrer les données des utilisateurs stockées sur leurs serveurs.

Sécurité d'iCloud Drive

iCloud Drive ajoute des clés basées sur le compte pour protéger les documents stockés dans iCloud. iCloud Drive divise et chiffre le contenu des fichiers, puis stocke ces blocs chiffrés à l'aide de services tiers. Les clés de contenu de fichier sont toutefois enveloppées par des clés d'enregistrement stockées avec les métadonnées iCloud Drive. Ces clés d'enregistrement sont à leur tour protégées par la clé de service iCloud Drive de l'utilisateur, laquelle est ensuite stockée avec son compte iCloud. Les utilisateurs ont accès aux métadonnées de leurs documents iCloud en s'authentifiant auprès du service iCloud, mais ils doivent également disposer de la clé de service iCloud Drive pour exposer les parties protégées du stockage iCloud Drive.

Sauvegarde iCloud Drive

iCloud permet également de sauvegarder quotidiennement des informations (telles que les réglages d'appareil, les données d'app, les photos et vidéos de la pellicule ainsi que les conversations de l'app Messages) par Wi-Fi. iCloud protège le contenu en le chiffrant lorsqu'il est envoyé par Internet, en le stockant dans un format chiffré et en utilisant des jetons sécurisés pour l'authentification. La sauvegarde iCloud n'est effectuée que si l'appareil est verrouillé, branché à une source d'alimentation et connecté à Internet par Wi-Fi. En raison du type de chiffrement utilisé dans iOS et iPadOS, la sauvegarde iCloud est conçue pour protéger les données tout en autorisant des sauvegardes et des restaurations incrémentales et sans surveillance.

Si des fichiers sont créés dans des classes de protection de données inaccessibles lorsque l'appareil est verrouillé, leurs clés par fichier sont chiffrées à l'aide des clés de classe provenant du conteneur de clés de la sauvegarde iCloud et en sauvegardant les fichiers sur iCloud dans leur état chiffré d'origine. Tous les fichiers sont chiffrés pendant le transport et, lors du stockage, à l'aide de clés basées sur le compte, comme décrit dans la section CloudKit.

Le conteneur de clés de la sauvegarde iCloud contient des clés asymétriques (Curve25519) pour les classes de protection des données qui sont inaccessibles lorsque l'appareil est verrouillé. La sauvegarde est stockée dans le compte iCloud de l'utilisateur et comprend une copie des fichiers de l'utilisateur et du conteneur de clés de la sauvegarde iCloud. Ce dernier est protégé par une clé aléatoire également stockée avec la sauvegarde. (Le mot de passe iCloud de l'utilisateur n'est pas utilisé pour le chiffrement, donc toute modification n'aura aucune incidence sur la validité des sauvegardes existantes.)

Bien que la base de données du trousseau de l'utilisateur soit sauvegardée sur iCloud, elle demeure protégée par une clé emmêlée avec l'UID. Cela permet de restaurer le trousseau uniquement sur son appareil d'origine afin que personne d'autre (pas même Apple) n'ait accès aux éléments du trousseau de l'utilisateur.

Lors de la restauration, les fichiers sauvegardés, le conteneur de clés de la sauvegarde iCloud et la clé du conteneur de clés sont récupérés à partir du compte iCloud de l'utilisateur. Le conteneur de clés de la sauvegarde iCloud est déchiffré au moyen de sa clé; les clés par fichier qu'il contient sont alors utilisées pour déchiffrer les fichiers de la sauvegarde, qui sont ensuite écrits en tant que nouveaux fichiers dans le système de fichiers, ce qui a pour conséquence de les chiffrer à nouveau en fonction de leur classe de protection de données.

Sécurité de la sauvegarde iCloud

Le contenu suivant est visé par la sauvegarde iCloud :

- Données sur la musique, les films, les émissions de télévision, les apps et les livres achetés. La sauvegarde iCloud d'un utilisateur inclut des informations sur le contenu acheté présent sur son appareil, mais pas le contenu même. Lorsque l'utilisateur effectue une restauration à partir d'une sauvegarde iCloud, le contenu acheté est téléchargé automatiquement à partir de l'iTunes Store, de l'App Store, de l'app Apple TV ou d'Apple Books. Certains types de contenus ne sont pas téléchargés automatiquement dans tous les pays ou régions, et les achats antérieurs pourraient ne pas être disponibles s'ils ont été remboursés ou s'ils ne sont plus disponibles dans la boutique. L'historique complet des achats est associé à l'identifiant Apple de l'utilisateur.

- Photos et vidéos sur les appareils de l'utilisateur. Notez que si l'utilisateur active Photos iCloud sous iOS 8.1 ou version ultérieure, sous iPadOS 13.1 ou version ultérieure, ou sous OS X 10.10.3 ou version ultérieure, ses photos et vidéos sont déjà stockées sur iCloud; elles ne sont donc pas incluses dans sa sauvegarde iCloud.
- Contacts, événements de calendrier, rappels et notes.
- Réglages de l'appareil.
- Données des apps.
- Écran d'accueil et organisation des apps.
- Configuration de HomeKit.
- Données de la fiche médicale.
- Mot de passe de la messagerie vocale visuelle (nécessite la carte SIM utilisée au moment de la sauvegarde).
- iMessage, clavardage commercial, messages texte (SMS) et messages MMS (nécessite la carte SIM utilisée au moment de la sauvegarde).

Lorsque Messages est activée dans iCloud, iMessage, le clavardage commercial ainsi que les messages texte et MMS sont supprimés de la sauvegarde iCloud de l'utilisateur pour être plutôt stockés dans un conteneur CloudKit chiffré de bout en bout pour Messages. La sauvegarde iCloud de l'utilisateur conserve une clé de ce conteneur. Si l'utilisateur désactive par la suite la sauvegarde iCloud, cette clé du conteneur est renouvelée, la nouvelle clé est stockée uniquement dans le trousseau iCloud (inaccessible à Apple et aux tiers), et il est impossible de déchiffrer les nouvelles données inscrites dans le conteneur à l'aide de l'ancienne clé.

La clé utilisée pour restaurer les messages dans la sauvegarde iCloud est placée à deux emplacements : dans le trousseau iCloud et une sauvegarde dans CloudKit. La sauvegarde dans CloudKit est effectuée si la sauvegarde iCloud est activée et restaurée sans condition, que l'utilisateur restaure une sauvegarde iCloud ou non.

Chiffrement de bout en bout CloudKit

De nombreux services Apple, répertoriés dans l'article de l'assistance Apple Présentation de la sécurité iCloud, ont recours au chiffrement de bout en bout avec une clé de service CloudKit protégée par la synchronisation du trousseau iCloud. Pour ces conteneurs CloudKit, la hiérarchie de clés provient du trousseau iCloud et, par conséquent, elle présente les mêmes caractéristiques de sécurité (c'est-à-dire que les clés sont accessibles uniquement par les appareils approuvés de l'utilisateur et non par Apple ni par un tiers). Si l'accès aux données du trousseau iCloud est perdu, les données dans CloudKit sont réinitialisées, et, si des données sont accessibles sur l'appareil local approuvé, elles sont téléchargées de nouveau vers CloudKit. Pour en savoir plus, consultez la section Sécurité de l'autorité de séquestre pour le trousseau iCloud.

Messages dans iCloud a aussi recours au chiffrement de bout en bout CloudKit avec une clé de service CloudKit protégée par la synchronisation du trousseau iCloud. Si l'utilisateur a activé la sauvegarde iCloud, la clé de service CloudKit utilisée pour Messages dans le conteneur iCloud est sauvegardée dans iCloud pour permettre à l'utilisateur de récupérer ses messages, même s'il perd l'accès au trousseau iCloud et à ses appareils approuvés. Cette clé de service iCloud est renouvelée lorsque l'utilisateur désactive la sauvegarde iCloud.

Situation	Options de récupération de l’utilisateur pour le chiffrement de bout en bout CloudKit
Accès à un appareil approuvé	Récupération des données possible via l’appareil approuvé ou le trousseau iCloud
Aucun appareil approuvé	Récupération des données possible uniquement via le trousseau iCloud
Sauvegarde iCloud activée et accès à un appareil approuvé	Récupération des données possible via la sauvegarde i Cloud, l’appareil approuvé ou le trousseau iCloud
Sauvegarde iCloud activée; aucun appareil approuvé	Récupération des données possible via la sauvegarde i Cloud ou le trousseau iCloud
Sauvegarde iCloud désactivée et accès à un appareil approuvé	Récupération des données possible via l’appareil approuvé ou le trousseau iCloud
Sauvegarde désactivée; aucun appareil approuvé	Récupération des données possible uniquement via le trousseau iCloud

Gestion des codes et des mots de passe

Aperçu de la sécurité du mot de passe

iOS, iPadOS et macOS permettent aux utilisateurs de s’authentifier simplement auprès des apps et des sites Web tiers qui utilisent des mots de passe. La meilleure façon de gérer des mots de passe est de ne pas avoir à en utiliser. La fonction Connexion avec Apple permet aux utilisateurs de se connecter à des apps tierces et à des sites Web sans avoir à créer ou à gérer un compte ou un mot de passe supplémentaire tout en protégeant la connexion à l’aide de l’authentification à deux facteurs pour l’identifiant Apple. Pour les sites qui ne prennent pas en charge Connexion avec Apple, la fonction de génération automatique de mots de passe robustes offre la création, la synchronisation et la saisie automatiques de mots de passe complexes et uniques pour les sites et les apps. Dans iOS et iPadOS, les mots de passe sont enregistrés dans un trousseau de remplissage automatique des mots de passe qui est contrôlé par l’utilisateur et qui se gère dans Réglages > Mots de passe.

Sous macOS, les mots de passe enregistrés peuvent être gérés dans les préférences Mots de passe de Safari. Ce système peut aussi être utilisé pour synchroniser les mots de passe que l’utilisateur crée manuellement.

Sécurité de Connexion avec Apple

Connexion avec Apple est une solution axée sur la confidentialité qui peut remplacer les autres systèmes d’authentification unique. Cette fonction offre la commodité et l’efficacité d’une connexion en un toucher tout en donnant à l’utilisateur plus de transparence et plus de contrôle sur ses renseignement personnels.

Connexion avec Apple permet à l'utilisateur de configurer un compte et de se connecter à des apps ou à des sites Web à l'aide de l'identifiant Apple qu'il possède déjà. Les apps peuvent uniquement demander le nom et l'adresse courriel de l'utilisateur lors de la configuration d'un compte, et l'utilisateur a toujours un choix : partager son adresse courriel personnelle avec l'app ou préserver sa confidentialité en utilisant plutôt le nouveau service de relais courriel privé d'Apple. Ce service partage une adresse courriel anonymisée unique qui redirige les courriels vers l'adresse personnelle de l'utilisateur afin qu'il puisse continuer de recevoir des communications utiles de la part des développeurs, tout en maintenant un certain degré de confidentialité et de contrôle sur ses informations personnelles.

Connexion avec Apple est conçu pour la sécurité. Chaque utilisateur de Connexion avec Apple doit activer l'authentification à deux facteurs pour son identifiant Apple, ce qui lui permet de sécuriser non seulement son identifiant Apple, mais aussi ses comptes auprès des apps. Par ailleurs, Apple a développé un signal antifraude à des fins de confidentialité et l'a intégré à Connexion avec Apple. Le signal donne aux développeurs la certitude que les nouveaux utilisateurs acquis sont de véritables personnes, et non des robots ou des comptes exécutés par des scripts.

Génération automatique de mots de passe robustes

Lorsque le trousseau iCloud est activé, iOS, iPadOS et macOS créent des mots de passe robustes, aléatoires et uniques quand les utilisateurs s'inscrivent sur un site Web ou lorsqu'ils modifient leur mot de passe de connexion à un site Web dans Safari. Sous iOS et iPadOS, la génération automatique de mots de passe robustes est également proposée dans les apps Les utilisateurs doivent eux-mêmes refuser l'utilisation de ces mots de passe. Les mots de passe générés sont enregistrés dans le trousseau et synchronisés entre les appareils à l'aide du trousseau iCloud, s'il est activé.

Par défaut, les mots de passe générés par iOS et iPadOS contiennent 20 caractères. Ils renferment 1 chiffre, 1 lettre majuscule, 2 traits d'union et 16 lettres minuscules. Ces mots de passe générés sont forts et possèdent une entropie de 71 bits.

Les mots de passe sont générés selon une heuristique qui détermine si l'expérience d'un champ de mot de passe est pour sa création. Si l'heuristique ne reconnaît pas un mot de passe lié au contexte lors de la création du mot de passe en question, les développeurs de l'app peuvent régler `UITextContentType.newPassword` dans leur champ de texte, et les développeurs Web peuvent définir `autocomplete= "new-password"` dans leurs éléments <input>.

Pour contribuer à garantir que les mots de passe générés sont compatibles avec les services pertinents, les apps et les sites Web peuvent fournir des règles. Les développeurs fournissent ces règles à l'aide de `UITextInputPasswordRules` ou de l'attribut `passwordrules` dans leurs éléments d'intrant. Les appareils génèrent ensuite le mot de passe le plus fort possible dans le respect de ces règles.

Sécurité du remplissage automatique des mots de passe

Le remplissage automatique des mots de passe remplit automatiquement les informations d'identification stockées dans le trousseau. Le gestionnaire de mots de passe du trousseau iCloud et le remplissage automatique des mots de passe offrent les fonctionnalités suivantes :

- remplissage des informations d’identification dans les apps et sur les sites Web;
- création de mots de passe robustes;
- enregistrement des mots de passe dans les apps et sur les sites Web dans Safari;
- partage sécuritaire des mots de passe avec les contacts de l’utilisateur;
- transmission des mots de passe à une Apple TV à proximité qui demande des informations d’identification.

La création et l’enregistrement de mots de passe dans les apps ainsi que la transmission des mots de passe à l’Apple TV sont disponibles uniquement sous iOS et iPadOS.

Remplissage automatique des mots de passe dans les apps

iOS et iPadOS permettent aux utilisateurs de saisir les noms d’utilisateur et les mots de passe enregistrés dans les champs d’identification des apps, comme le fait le remplissage automatique de mot de passe dans Safari. Sous iOS et iPadOS, les utilisateurs le font en touchant une touche de suggestion dans la barre QuickType du clavier logiciel. Sous macOS, pour les apps conçues avec Mac Catalyst, un menu déroulant « Mots de passe » s’affiche sous les champs d’identification.

Lorsqu’une app est fortement associée à un site Web qui utilise le même mécanisme d’association entre app et site Web, exécuté par le même fichier apple-app-site-association, la barre QuickType sous iOS et iPadOS et le menu déroulant sous macOS suggèrent directement les informations d’identification pour l’app, si elles sont enregistrées dans le trousseau de remplissage automatique des mots de passe. Ainsi, les utilisateurs peuvent choisir de divulguer les informations d’identification enregistrées dans Safari aux apps qui partagent les mêmes propriétés de sécurité, sans que ces apps aient à adopter une API.

Le remplissage automatique des mots de passe n’expose aucune information d’identification à une app avant que l’utilisateur y consente. Les listes d’informations d’identification sont extraites du processus de l’app.

Lorsqu’une app et un site Web ont une relation de confiance et qu’un utilisateur soumet des informations d’identification dans une app, iOS et iPadOS peuvent demander à l’utilisateur d’enregistrer ces informations dans le trousseau de remplissage automatique des mots de passe pour les utiliser plus tard.

Accès des apps aux mots de passe enregistrés

Les apps iOS, iPadOS et macOS peuvent demander l’aide du trousseau de remplissage automatique des mots de passe pour connecter un utilisateur avec ASAuthorizationPasswordProvider et SecAddSharedWebCredential. Le fournisseur du mot de passe et sa demande peuvent être utilisés conjointement avec Connexion avec Apple afin que la même API puisse aider l’utilisateur à se connecter à une app, peu importe si son compte est doté d’un mot de passe ou créé par Connexion avec Apple.

Les apps peuvent accéder aux mots de passe enregistrés uniquement si le développeur de l'app et l'administrateur du site Web donnent tous deux leur approbation, et si l'utilisateur donne son accord. Les développeurs d'apps expriment leur intention d'accéder aux mots de passe enregistrés par Safari en incluant une déclaration d'autorisation dans leur app. Cette déclaration répertorie les noms de domaine complets des sites Web associés, et les sites Web doivent avoir sur leur serveur un fichier contenant la liste des identifiants uniques des apps approuvées par Apple.

Lorsqu'une app avec le droit com.apple.developer.associated-domains est installée, iOS et iPadOS envoient une requête TLS à chaque site Web répertorié pour demander un des fichiers suivants :

- apple-app-site-association
- .well-known/apple-app-site-association

Si le fichier fait état de l'identifiant de l'app en cours d'installation, iOS et iPadOS marquent alors le site Web et l'app comme ayant une relation de confiance. L'établissement d'une relation de confiance est nécessaire pour que les appels à ces deux API entraînent la présentation d'une invite à l'utilisateur, qui doit alors donner son accord avant qu'un mot de passe ne soit transmis à l'app, mis à jour ou supprimé.

Avis relatifs à la sécurité des mots de passe

Aperçu

La liste de remplissage automatique des mots de passe sous iOS, iPadOS et macOS indique les mots de passe enregistrés par l'utilisateur qui sont réutilisés sur d'autres sites Web, les mots de passe qui sont considérés comme faibles et ceux qui ont été compromis dans le cadre d'une fuite de données.

L'utilisation du même mot de passe pour plus d'un service peut rendre ces comptes vulnérables en cas d'attaque par bourrage d'identifiants. En cas de fuite de mots de passe après l'infiltration d'un service, les assaillants peuvent essayer les mêmes informations d'identification sur d'autres services pour compromettre davantage de comptes. Les mots de passe qui sont utilisés sur plusieurs domaines différents sont marqués comme *réutilisés*.

Les mots de passe sont marqués comme *faibles* s'ils peuvent être facilement devinés par un assaillant. iOS, iPadOS et macOS détectent les tactiques couramment utilisées pour créer des mots de passe mémorisables, comme l'utilisation de mots du dictionnaire, la substitution de caractères (« m0tdep4sse » au lieu de « motdepasse »), l'utilisation de séquences présentes sur le clavier (« q12we34r » sur un clavier QWERTY) ou l'utilisation de séquences répétées (« 123123 »). Ces séquences sont souvent employées pour créer des mots de passe qui respectent les exigences minimales pour les services, mais sont aussi souvent employées par les assaillants qui tentent d'obtenir un mot de passe par une attaque en force.

Comme de nombreux services exigent expressément un NIP à quatre ou à six chiffres, ces codes courts sont évalués selon des règles différentes. Les NIP sont considérés comme faibles s'ils sont un des codes les plus courants, s'il s'agit d'une séquence croissante ou décroissante comme « 1234 » ou « 8765 », ou s'ils suivent un schéma de répétition comme « 123123 » ou « 123321 ».

Les mots de passe sont signalés comme *associés à une fuite de données* si la fonction de surveillance des mots de passe est en mesure de vérifier qu'ils ont été reconnus dans une fuite de données. Pour en savoir plus, consultez la section Surveillance des mots de passe.

Les mots de passe faibles, réutilisés ou associés à une fuite de données sont répertoriés soit dans la liste des mots de passe (macOS), soit dans l'interface dédiée aux avis relatifs à la sécurité (iOS et iPadOS). Si l'utilisateur se connecte à un site Web dans Safari à l'aide d'un mot de passe déjà enregistré qui est très faible ou qui a été compromis dans le cadre d'une fuite de données, il reçoit une alerte qui l'encourage fortement à utiliser un mot de passe robuste généré automatiquement.

Mise à niveau de la sécurité d'authentification des comptes au moyen d'extensions de modification de l'authentification des comptes

Les apps qui implémentent une extension de modification de l'authentification des comptes peuvent proposer à l'utilisateur de mettre facilement à niveau le mot de passe associé au compte de l'app au moyen d'un simple bouton qui permet d'utiliser Connexion avec Apple ou un mot de passe robuste généré automatiquement à la place du mot de passe actuel. Ce point d'extension est disponible sous iOS et iPadOS.

Si une app a implémenté le point d'extension et qu'elle est installée sur l'appareil, son utilisateur verra les options de mise à niveau lorsqu'il consultera les avis relatifs à la sécurité pour les informations d'identification associées à l'app dans le gestionnaire de mots de passe du trousseau iCloud, dans Réglages. Les mises à niveau sont également proposées lorsque l'utilisateur se connecte à l'app au moyen d'informations d'identification qui présentent un risque. Les apps sont en mesure de demander au système de ne pas afficher les options de mise à niveau une fois l'utilisateur connecté. En utilisant la nouvelle API AuthenticationServices, les apps peuvent appeler leurs extensions et procéder elles-mêmes aux mises à niveau, idéalement à partir des réglages du compte ou de l'écran de gestion du compte dans l'app.

Les apps peuvent choisir de prendre en charge les mises à niveau vers un mot de passe robuste, les mises à niveau vers Connexion avec Apple, ou les deux. Lorsqu'une mise à niveau vers un mot de passe robuste a lieu, le système génère automatiquement un mot de passe robuste pour l'utilisateur. Si nécessaire, l'app peut fournir des règles personnalisées de mot de passe qui devront être suivies pour générer le nouveau mot de passe. Lorsqu'un utilisateur choisi pour un compte donné d'utiliser Connexion avec Apple au lieu de son mot de passe, le système fournit de nouvelles données d'identification Connexion avec Apple à l'extension pour les associer au compte. L'adresse courriel associée à l'identifiant Apple de l'utilisateur ne fait pas partie des informations transmises. Après une mise à niveau réussie vers Connexion avec Apple, le système supprime le mot de passe utilisé précédemment du trousseau de l'utilisateur si ces informations d'identification y étaient enregistrées.

Les extensions de modification de l'authentification des comptes sont en mesure d'effectuer d'autres authentifications de l'utilisateur avant de procéder à la mise à niveau. Pour les mises à niveau qui proviennent du gestionnaire de mots de passe ou qui ont commencé après que l'utilisateur s'est connecté à une app, l'extension transmet le nom d'utilisateur et le mot de passe correspondant pour que la mise à niveau du compte ait lieu. Pour les mises à niveau effectuées directement dans l'app, seul le nom d'utilisateur est fourni. Si l'extension requiert une authentification plus approfondie de l'utilisateur, elle peut demander d'afficher une interface utilisateur personnalisée avant de procéder à la mise à niveau. Une telle interface a pour but de demander à l'utilisateur d'entrer un second facteur d'authentification pour autoriser la mise à niveau.

Surveillance des mots de passe

La surveillance des mots de passe est une fonctionnalité qui compare les mots de passe stockés le trousseau de remplissage automatique de mots de passe de l'utilisateur avec une liste préparée avec soin et continuellement mise à jour de mots de passe connus pour avoir été exposés dans le cadre de fuites de données de différentes organisations présentes en ligne. Si la fonctionnalité est activée, le protocole de surveillance compare en permanence les mots de passe du trousseau de remplissage automatique de mots de passe de l'utilisateur avec cette liste soigneusement élaborée.

Fonctionnement de la surveillance

L'appareil de l'utilisateur effectue continuellement des vérifications circulaires des mots de passe de l'utilisateur et soumet les requêtes à un intervalle indépendant pour veiller à ce que les états de vérification soient à jour en tenant compte de la liste actuelle de mots de passe divulgués. Afin de contribuer à éviter la fuite d'informations quant au nombre de mots de passe uniques dont un utilisateur dispose, les demandes sont consolidées et soumises en parallèle. Un nombre fixe de mots de passe est vérifié en parallèle lors de chaque vérification. Des mots de passe aléatoires sont générés et ajoutés aux requêtes pour compenser la différence si le nombre de mots de passe de l'utilisateur est inférieur à ce nombre fixe.

Mise en correspondance des mots de passe

La mise en correspondance des mots de passe s'effectue en deux phases. Les mots de passe les plus communs parmi ceux qui ont été divulgués dans le cadre de fuites de données sont répertoriés dans une liste locale sur l'appareil de l'utilisateur. Si le mot de passe de l'utilisateur figure sur cette liste, l'utilisateur est immédiatement alerté sans interaction externe. Cela vise à garantir qu'aucune information n'est divulguée sur les mots de passe les plus vulnérables d'un utilisateur en raison d'une fuite de mots de passe.

Si le mot de passe ne figure pas dans cette liste, il est comparé avec les mots de passe divulgués moins fréquemment.

Comparaison des mots de passe des utilisateurs avec une liste préparée

La vérification d'un mot de passe qui ne figure pas dans la liste locale requiert des interactions avec les serveurs d'Apple. Afin de veiller à ce que les véritables mots de passe des utilisateurs ne soient pas envoyés à Apple, une forme d'*intersection d'ensembles cryptographiques confidentiels* est déployée pour comparer les mots de passe avec un large ensemble de mots de passe divulgués. Cela vise à garantir que peu d'informations sont partagées avec Apple quant aux mots de passe dont le risque de violation est moindre. Pour le mot de passe d'un utilisateur, ces informations sont limitées à un préfixe de 15 bits d'un hachage cryptographique. La suppression des mots de passe les plus fréquemment divulgués de ce processus interactif, en utilisant la liste locale des mots de passe divulgués les plus communs, réduit le delta en fréquence relative des mots de passe qui figurent dans les compartiments du service Web tout en empêchant quiconque de deviner les mots de passe des utilisateurs à partir de ces recherches.

Le protocole sous-jacent divise la liste des mots de passe traités (la liste contient environ 1,5 milliard de mots de passe au moment où nous rédigeons ce guide) en 2^{15} compartiments différents. Les 15 premiers bits de la valeur de hachage SHA256 du mot de passe déterminent le compartiment auquel le mot de passe est assigné. Par ailleurs, chaque mot de passe divulgué (pw) est associé à un point de courbe elliptique sur la courbe NIST P256 : $P_{pw} =$ $\cdot H_{SWU}(pw)$, où est une clé aléatoire secrète connue uniquement par Apple, et H_{SWU} est une fonction d'oracle aléatoire qui met les mots de passe en correspondance avec des points de courbe selon la méthode Shallue–Van de Woestijne–Ulas. Cette transformation est conçue pour masquer informatiquement les valeurs des mots de passe et contribuer à empêcher la révélation de mots de passe ayant récemment fait l'objet d'une fuite par l'entremise de la surveillance des mots de passe.

Pour calculer l'intersection d'ensembles confidentiels, l'appareil de l'utilisateur détermine le compartiment auquel le mot de passe de l'utilisateur appartient en utilisant λ, le préfixe de 15 bits de SHA256(upw), où upw est l'un des mots de passe de l'utilisateur. L'appareil génère sa propre constante aléatoire, β, puis envoie le point $P_c = \beta \cdot H_{SWU}(upw)$ au serveur accompagné d'une requête pour le compartiment qui correspond à λ. Ici, β masque les informations qui se rapportent au mot de passe de l'utilisateur et limite les informations issues du mot de passe à λ pour Apple. Enfin, le serveur reçoit le point envoyé par l'appareil de l'utilisateur, procède au calcul, $P_c =$ $\beta \cdot H_{SWU}(upw)$, et le renvoie à l'appareil accompagné du compartiment approprié des points : $B\lambda = \{ P_{pw} \mid$ SHA256(pw) commence avec le préfixe λ$\}$.

Les informations reçues permettent à l'appareil de calculer $B'_\lambda = \{\beta \cdot P_{pw} \mid P_{pw}$ $B_\lambda\}$, et s'il en résulte que P_c B'_λ, cela établit que le mot de passe de l'utilisateur a fait l'objet d'une fuite.

Envoi de mots de passe à d'autres utilisateurs ou appareils Apple

Enregistrement d'informations d'identification sur un autre appareil avec AirDrop

Lorsqu'iCloud est activé, les utilisateurs peuvent transférer par AirDrop des informations d'identification enregistrées, y compris les sites Web pour lesquels elles sont enregistrées, le nom d'utilisateur et le mot de passe, à un autre appareil. L'envoi d'informations d'identification avec AirDrop fonctionne toujours en mode Contacts uniquement, peu importe les réglages de l'utilisateur. Sur l'appareil récepteur, après le consentement de l'utilisateur, les informations d'identification sont stockées dans le trousseau de remplissage automatique des mots de passe de l'utilisateur.

Remplissage des informations d'identification dans les apps sur Apple TV

Le remplissage automatique des mots de passe est disponible pour remplir les informations d'identification dans les apps sur Apple TV. Lorsque l'utilisateur sélectionne un champ de texte pour un nom d'utilisateur ou un mot de passe sous tvOS, son Apple TV commence à diffuser une demande de remplissage automatique des mots de passe par Bluetooth faible énergie (BLE).

Tout iPhone, iPad ou iPod touch à proximité affiche un message invitant l'utilisateur à partager ses informations d'identification avec l'Apple TV. Voici comment la méthode de chiffrement est établie :

- Si l’appareil et Apple TV utilise le même compte iCloud, le chiffrement entre les appareils se produit automatiquement.
- Si l’appareil est connecté à un compte iCloud autre que celui utilisé par l’Apple TV, l’utilisateur est invité à établir une connexion chiffrée en utilisant un NIP. Pour recevoir cette invite, l’iPhone doit être déverrouillé et à proximité de la télécommande Siri Remote jumelée à l’Apple TV pour recevoir ce message.

Après l’établissement de la connexion chiffrée à l’aide du chiffrement de lien BLE, les informations d’identifications sont envoyées à l’Apple TV, et les champs de texte correspondants sont automatiquement remplis dans l’app.

Extensions de fournisseurs d’informations d’identification

Sous iOS, iPadOS et macOS, les utilisateurs peuvent désigner une app tierce participante comme fournisseuse d’informations d’identification pour le remplissage automatique des mots de passe dans les réglages Mots de passe (iOS et iPadOS) ou dans Préférences Système > Extensions (macOS). Ce mécanisme est fondé sur des extensions d’app. L’extension de fournisseurs d’informations d’identification doit fournir une interface pour la sélection des informations, et elle peut fournir des métadonnées qui se rapportent aux informations d’identification enregistrées afin qu’elles puissent être proposées directement dans la barre QuickType (iOS et iPadOS) ou dans les suggestions de remplissage automatique (macOS). Les métadonnées comprennent le site Web pour les informations d’identification et le nom d’utilisateur associé, mais pas son mot de passe. iOS, iPadOS et macOS communiqueront avec l’extension pour obtenir le mot de passe lorsque l’utilisateur choisira de remplir les informations d’identification dans une app ou sur un site Web dans Safari. Les métadonnées des informations d’identification sont stockées dans le conteneur de l’app du fournisseur et sont automatiquement supprimées lorsqu’une app est désinstallée.

Trousseau iCloud

Aperçu de la sécurité du trousseau iCloud

iCloud donne aux utilisateurs la possibilité de synchroniser de façon sécurisée leurs mots de passe avec plusieurs appareils iOS et iPadOS, et ordinateurs Mac sans divulguer ces informations à Apple. Outre la volonté de fournir un niveau de confidentialité et de sécurité supérieur, d’autres objectifs ont fortement influencé la conception et l’architecture du trousseau iCloud, comme la facilité d’utilisation et la possibilité de restaurer des trousseaux. Le trousseau iCloud consiste en deux services : la synchronisation du trousseau et sa récupération.

Apple a conçu le trousseau iCloud et la récupération du trousseau de telle sorte que les mots de passe d’un utilisateur demeurent protégés dans les situations suivantes :

- Le compte iCloud de l’utilisateur est compromis.
- iCloud a été compromis par un employé ou une attaque externe.
- Un tiers accède aux comptes utilisateur.

Intégration du gestionnaire de mots de passe au trousseau iCloud

iOS, iPadOS et macOS peuvent générer automatiquement des chaînes aléatoires robustes du point de vue cryptographique pour les utiliser comme mots de passe de comptes dans Safari. iOS et iPadOS peuvent aussi générer des mots de passe robustes pour les apps. Les mots de passe générés sont stockés dans le trousseau et synchronisés avec les autres appareils. Les éléments de trousseau sont transférés d'un appareil à l'autre en passant par les serveurs d'Apple, mais sont chiffrés de façon à ce que leur contenu ne puisse être lu ni par Apple ni par d'autres appareils.

Synchronisation sécurisée du trousseau

Lorsqu'un utilisateur active le trousseau iCloud pour la première fois, l'appareil établit un cercle de confiance et crée une identité de synchronisation pour lui-même. L'identité de synchronisation est constituée d'une clé privée et d'une clé publique. La clé publique de l'identité de synchronisation est placée dans le cercle, et ce dernier est signé deux fois : une première fois avec la clé privée de l'identité de synchronisation, et une deuxième fois avec une clé asymétrique sur courbe elliptique (avec P-256) dérivée du mot de passe du compte iCloud de l'utilisateur. Les paramètres utilisés pour créer la clé basée sur le mot de passe iCloud de l'utilisateur (sel et itérations aléatoires) sont également stockés avec le cercle.

Le cercle de synchronisation est placé dans l'iCloud de l'utilisateur

Le cercle de synchronisation signé est ensuite placé dans la zone de stockage clé-valeur d'iCloud de l'utilisateur. Il est impossible de lire ce cercle sans connaître le mot de passe iCloud de l'utilisateur, ou de le modifier de manière valide sans la clé privée de l'identité de synchronisation de son membre.

Lorsque l'utilisateur active le trousseau iCloud sur un autre appareil, le trousseau détecte dans iCloud que l'utilisateur possède un cercle de synchronisation précédemment établi dont il ne fait pas partie. L'appareil crée sa paire de clés d'identité de synchronisation, puis crée un ticket de candidature pour demander à devenir membre du cercle. Le ticket est constitué de la clé publique de l'identité de synchronisation de l'appareil; l'utilisateur est invité à s'authentifier à l'aide de son mot de passe iCloud. Les paramètres de génération de clé sur courbe elliptique sont récupérés à partir d'iCloud et permettent d'obtenir une clé destinée à signer le ticket de candidature. Enfin, le ticket de candidature est placé dans iCloud.

Ajout d'autres appareils de l'utilisateur au cercle de synchronisation

Lorsque le premier appareil constate qu'un ticket de candidature est arrivé, il demande à l'utilisateur de confirmer qu'un nouvel appareil demande à faire partie du cercle de synchronisation. L'utilisateur saisit son mot de passe iCloud, et le ticket de candidature est vérifié pour confirmer qu'il a été signé par la clé privée appropriée. Les utilisateurs qui ont généré la demande pour joindre le cercle peuvent maintenant le faire.

Lorsque l'utilisateur accepte d'ajouter le nouvel appareil au cercle, le premier appareil ajoute la clé publique du nouveau membre au cercle de synchronisation et la signe à nouveau avec son identité de synchronisation et la clé dérivée du mot de passe iCloud de l'utilisateur. Le nouveau cercle de synchronisation est alors placé dans iCloud, où il est signé de la même manière par le nouveau membre du cercle.

Il y a à présent deux membres du cercle de signature, et chacun possède la clé publique de son homologue. Ils commencent alors à s'échanger des éléments de trousseau individuels par l'entremise de l'espace de stockage clé-valeur d'iCloud ou à les stocker dans CloudKit, selon l'option qui convient le mieux à la situation. Si les deux membres du cercle possèdent le même élément, c'est l'élément présentant la date de modification la plus récente qui est synchronisé. Les éléments détenus par les deux membres et dont les dates de modification sont identiques sont ignorés. Chaque élément synchronisé est chiffré de façon à ne pouvoir être déchiffré que par un appareil faisant partie du cercle de confiance de l'utilisateur; les autres appareils ne peuvent pas le faire, ni Apple.

Cette procédure est répétée chaque fois que de nouveaux appareils se joignent au cercle de synchronisation. Ainsi, si un troisième appareil entre dans le cercle, le message de confirmation s'affiche sur les deux autres appareils de l'utilisateur, qui peut alors approuver le nouveau membre à partir de l'un de ces deux appareils. À mesure que de nouveaux appareils sont ajoutés, chacun d'entre eux est synchronisé avec le nouveau pour veiller à ce que tous les membres disposent des mêmes éléments de trousseau.

Synchronisation sélective

La totalité du trousseau n'est toutefois pas synchronisée. Certains éléments, comme les identités de VPN, sont propres à un appareil et ne devraient pas quitter celui-ci. Seuls les éléments possédant l'attribut `kSecAttrSynchronizable` sont synchronisés. Apple a défini cet attribut pour les données d'utilisateur de Safari (notamment les noms d'utilisateur, les mots de passe et les numéros de carte de crédit) ainsi que pour les mots de passe Wi-Fi et les clés de chiffrement HomeKit.

De plus, les éléments de trousseau ajoutés par des apps tierces ne sont pas synchronisés par défaut. Les développeurs doivent définir l'attribut `kSecAttrSynchronizable` lorsqu'ils ajoutent des éléments au trousseau.

Récupération sécurisée du trousseau iCloud

Le trousseau iCloud confie les données du trousseau des utilisateurs à Apple *sans* lui permettre de lire les mots de passe et autres données qu'il contient. Elle offre aussi à l'utilisateur un filet de sécurité contre la perte de données, même s'il ne possède qu'un seul appareil. Cela s'avère particulièrement important lorsque Safari est utilisé pour générer des mots de passe robustes et aléatoires pour des comptes Web, car le trousseau constitue le seul endroit où sont enregistrés ces mots de passe.

La récupération du trousseau repose sur l'authentification secondaire et sur un service sécurisé d'autorité de séquestre créé spécifiquement par Apple pour soutenir cette fonctionnalité. Le trousseau de l'utilisateur est chiffré à l'aide d'un mot de passe complexe, et le service d'autorité de séquestre fournit une copie du trousseau uniquement si certaines conditions strictes sont remplies.

Utilisation d'une authentification secondaire

Il existe plusieurs façons de définir un mot de passe fort :

- Si l'authentification à deux facteurs est activée pour le compte de l'utilisateur, le code de l'appareil est utilisé pour récupérer un trousseau stocké sous séquestre.

- Si l’authentification à deux facteurs n’est pas configurée, l’utilisateur est invité à créer un code de sécurité iCloud en fournissant un code à six chiffres. Sinon, sans l’authentification à deux facteurs, les utilisateurs peuvent spécifier leur propre code plus long ou laisser leur appareil créer automatiquement un code de chiffrement aléatoire qu’ils peuvent ensuite enregistrer et conserver en lieu sûr.

Processus de stockage sous séquestre du trousseau

Une fois le code établi, le trousseau est stocké sous séquestre auprès d’Apple. L’appareil iOS, iPadOS ou macOS exporte d’abord une copie du trousseau de l’utilisateur, puis chiffre cette copie en l’enveloppant avec des clés dans un conteneur de clés asymétrique et la place dans la zone de stockage clé-valeur d’iCloud de l’utilisateur. Le conteneur de clés est enveloppé à l’aide du code de sécurité iCloud de l’utilisateur et de la clé publique de la grappe de modules de sécurité matériels (HSM, Hardware Security Modules) destinée à envoyer l’enregistrement à l’autorité de séquestre. Ce dernier devient alors l’enregistrement iCloud sous séquestre de l’utilisateur. Les comptes HSA2 offrent le même niveau de protection : le trousseau, qui est également stocké dans CloudKit, est enveloppé pour échanger les clés qui sont récupérables uniquement avec le contenu de l’enregistrement iCloud sous séquestre.

Remarque : Si l’utilisateur décide d’accepter un code de sécurité de chiffrement aléatoire au lieu d’indiquer son propre code constitué d’une série de quatre chiffres, aucun enregistrement stocké sous séquestre n’est nécessaire. C’est plutôt le code de sécurité iCloud qui est utilisé pour protéger directement la clé aléatoire.

En plus d’établir un code de sécurité, les utilisateurs doivent enregistrer un numéro de téléphone. Cela offre un second niveau d’authentification pour récupérer le trousseau. L’utilisateur reçoit un SMS auquel il doit répondre afin de procéder à la récupération.

Sécurité de l’autorité de séquestre pour le trousseau iCloud

iCloud offre une infrastructure sécurisée pour le stockage sous séquestre du trousseau afin de contribuer à garantir que seuls les utilisateurs et les appareils autorisés puissent effectuer une récupération. Sur le plan topologique, des grappes de modules de sécurité matériels (HSM, Hardware Security Modules) sont placées derrière iCloud pour protéger les enregistrements stockés sous séquestre. Comme décrit précédemment, chacun d’eux possède une clé utilisée pour chiffrer les enregistrements stockés sous séquestre placés sous sa garde.

Pour récupérer un trousseau, les utilisateurs doivent s’authentifier avec leur nom d’utilisateur et leur mot de passe iCloud et répondre à un message texte envoyé à leur numéro de téléphone enregistré. Ils doivent ensuite également saisir leur code de sécurité iCloud. La grappe de HSM vérifie que l’utilisateur connaît son code de sécurité iCloud grâce au protocole SRP (Secure Remote Password); le code lui-même n’est pas envoyé à Apple. Chaque membre de la grappe vérifie indépendamment que l’utilisateur n’a pas dépassé le nombre maximal de tentatives autorisées de récupération de son enregistrement (voir ci-dessous). Si cela est confirmé par une majorité de membres, l’enregistrement stocké sous séquestre est débloqué et envoyé à l’appareil de l’utilisateur.

L’appareil utilise ensuite le code de sécurité iCloud pour débloquer la clé aléatoire utilisée pour chiffrer le trousseau de l’utilisateur. Avec cette clé, le trousseau récupéré à partir de CloudKit et de la zone de stockage clé-valeur d’iCloud est déchiffré, puis restauré sur l’appareil. iOS, iPadOS et macOS autorisent uniquement 10 tentatives pour authentifier et récupérer un enregistrement sous séquestre. Après plusieurs tentatives manquées, l’enregistrement est verrouillé, et l’utilisateur doit appeler l’assistance Apple pour pouvoir effectuer des tentatives supplémentaires. Après la 10e tentative manquée, la grappe de HSM détruit l’enregistrement stocké sous séquestre, et le trousseau est perdu définitivement. Cette règle constitue une protection efficace contre les tentatives de récupération de l’enregistrement en force, mais les données du trousseau sont sacrifiées.

Ces politiques sont codées dans le programme interne de la grappe de HSM. Les cartes d’accès administratif permettant de modifier le programme interne ont été détruites. Toute tentative de modifier le programme interne ou d’accéder à la clé privée entraîne la suppression de celle-ci par la grappe de HSM. Dans ce cas, le propriétaire de chaque trousseau protégé par la grappe reçoit un message lui annonçant la perte de son enregistrement stocké sous séquestre. Il a alors la possibilité de se réinscrire au service.

Apple Pay

Aperçu de la sécurité d’Apple Pay

Grâce à Apple Pay, les utilisateurs peuvent se servir de tout appareil iPhone, iPad, Mac ou Apple Watch prenant en charge cette fonctionnalité pour effectuer de manière simple, sûre et confidentielle des paiements en magasin, dans les apps et sur le Web avec Safari. Ils peuvent également ajouter à Apple Wallet les cartes de transport et les cartes étudiantes compatibles. Ce système convivial repose sur des fonctionnalités de sécurité intégrées aux composants et aux logiciels.

Apple Pay est aussi conçu pour protéger les renseignements personnels de l’utilisateur. Et l’app ne conserve aucune donnée de transaction qui pourrait permettre d’identifier l’utilisateur. Les opérations de paiement sont réalisées entre l’utilisateur, le vendeur et l’émetteur de la carte.

Sécurité des composants Apple Pay

Secure Element

Le Secure Element est une puce certifiée, conforme aux normes de l’industrie, exécutant la plateforme Java Card, laquelle satisfait aux exigences du secteur financier pour les paiements électroniques. Le circuit intégré du Secure Element et la plateforme Java Card sont certifiés conformément au processus d’évaluation de la sécurité EMVCo. Une fois l’évaluation de la sécurité réussie, EMVCo délivre un certificat unique de circuit intégré et de plateforme.

Le circuit intégré du Secure Element est certifié conformément à la norme des Critères communs.

Contrôleur CCP

Le contrôleur CCP gère les protocoles de communication en champ proche et achemine la communication entre le processeur d'application et le Secure Element, et entre le Secure Element et le terminal de point de vente.

Apple Wallet

Apple Wallet permet d'ajouter et de gérer des cartes de crédit, de débit et de magasin, et de réaliser des paiements avec Apple Pay. Les utilisateurs peuvent y consulter leurs cartes et d'autres renseignements fournis par l'émetteur de leur carte, comme la politique de confidentialité de celui-ci, les dernières transactions et plus encore. Les utilisateurs peuvent également ajouter des cartes à Apple Pay dans :

- Assistant Réglages et Réglages sous iOS et iPadOS;
- l'app Watch pour l'Apple Watch;
- Wallet et Apple Pay dans Préférences Système sur les ordinateurs Mac dotés de Touch ID.

Par ailleurs, Apple Wallet permet aux utilisateurs d'ajouter et de gérer des cartes de transport, de fidélité et d'embarquement, des billets, des cartes-cadeaux, des cartes étudiantes et plus encore.

Secure Enclave

Sur iPhone, iPad, Apple Watch et les ordinateurs Mac dotés de Touch ID, le Secure Enclave gère le processus d'authentification et permet l'exécution des opérations de paiement.

Sur Apple Watch, l'appareil doit être déverrouillé, et l'utilisateur doit appuyer deux fois sur le bouton latéral. Le double-clic est détecté et transmis directement au Secure Element ou au Secure Enclave (selon le cas) sans passer par le processeur d'application.

Serveurs Apple Pay

Les serveurs Apple Pay gèrent la configuration ainsi que le transfert des cartes étudiantes, de paiement et de transport dans l'app Wallet. Les serveurs gèrent également les numéros de compte d'appareil stockés dans le Secure Element. Ils communiquent à la fois avec l'appareil et avec les serveurs des réseaux de paiement ou des émetteurs de cartes. Les serveurs Apple Pay sont également chargés de rechiffrer les informations d'identification de paiement pour les paiements réalisés dans les apps ou sur le Web.

Utilisation du Secure Element et du contrôleur CCP par Apple Pay

Secure Element

Le Secure Element renferme un applet spécifiquement conçu pour gérer Apple Pay. Il comporte également des applets certifiés par les réseaux de paiement ou les émetteurs de cartes. Les données de cartes de crédit, de débit ou prépayées sont transmises par le réseau de paiement ou par l'émetteur de la carte à ces applets sous forme chiffrée à l'aide de clés connues uniquement du réseau de paiement ou de l'émetteur de la carte et du domaine de sécurité des applets de paiement. Ces données sont stockées dans les applets et protégées à l'aide des fonctionnalités de sécurité du Secure Element. Lors d'une transaction, le terminal communique directement avec le Secure Element au moyen du contrôleur de communication en champ proche (CCP) par l'entremise d'un bus matériel dédié.

Contrôleur CCP

En tant que passerelle vers le Secure Element, le contrôleur CCP veille à ce que toutes les opérations de paiement sans contact soient réalisées par un terminal de point de vente situé à proximité immédiate de l'appareil. Seules les demandes de paiement émanant d'un terminal dans le champ sont considérées comme des transactions sans contact par le contrôleur CCP.

Une fois le paiement par carte prépayée, de crédit ou de débit (y compris les cartes de magasin) autorisé par le détenteur de la carte à l'aide de Touch ID, de Face ID ou d'un code, ou en appuyant deux fois sur le bouton latéral d'une Apple Watch déverrouillée, les réponses sans contact préparées par les applets de paiement dans le Secure Element sont acheminées exclusivement vers le champ CCP par le contrôleur. Les détails de l'autorisation de paiement pour les transactions de paiement sans contact sont donc transmis uniquement au champ CCP local et ne sont jamais divulgués au processeur d'application. Par contre, pour les paiements réalisés dans les apps et en ligne, ils sont acheminés vers le processeur d'application puis, après chiffrement par le Secure Element, vers le serveur Apple Pay.

Cartes de crédit, cartes de débit et cartes prépayées

Aperçu de la sécurité en matière de transfert de cartes

Lorsqu'un utilisateur ajoute une carte de crédit, de débit ou prépayée (ou la carte d'un magasin) à Apple Wallet, Apple envoie de façon sécurisée les données de celle-ci, ainsi que d'autres informations concernant le compte et l'appareil de l'utilisateur, à l'émetteur de la carte ou au fournisseur de services autorisé de l'émetteur de la carte. À l'aide de ces informations, l'émetteur de cartes décide d'approuver ou non l'ajout de la carte à Apple Wallet.

Dans le cadre du processus de transfert de cartes, Apple Pay utilise trois appels côté serveur pour communiquer avec l'émetteur de cartes ou le réseau : Champs obligatoires, Vérification de carte et Liaison et transfert. L'émetteur de la carte ou le réseau utilise ces appels pour vérifier, approuver et ajouter des cartes à Apple Wallet. Ces sessions client-serveur utilisent le protocole TLS 1.2 pour transférer les données.

Le numéro complet de la carte n'est stocké ni sur l'appareil ni sur les serveurs d'Apple Pay. Au lieu de cela, un numéro de compte de l'appareil est créé, chiffré, puis stocké dans le Secure Element. Ce numéro de compte de l'appareil est unique et chiffré de telle façon qu'Apple ne peut pas y accéder. Le numéro de compte de l'appareil étant unique et différent de la plupart des numéros de carte de paiement, l'émetteur de la carte ou le réseau de paiement peut empêcher son utilisation sur une carte à piste magnétique, par téléphone ou sur des sites Web. Le numéro de compte de l'appareil dans le Secure Element n'est jamais stocké sur les serveurs Apple Pay ni sauvegardé dans iCloud et il est isolé des appareils iOS, iPadOS et watchOS, ainsi que des ordinateurs Mac dotés de Touch ID.

Les cartes utilisées avec l'Apple Watch sont transférées pour Apple Pay via l'app Watch sur l'iPhone ou l'app pour iPhone des émetteurs de cartes. L'Apple Watch doit se trouver à portée du signal Bluetooth pour l'ajout d'une carte. Les cartes sont enregistrées expressément pour l'utilisation avec l'Apple Watch et ont leurs propres numéros de compte de l'appareil, qui sont stockés dans le Secure Element sur l'Apple Watch.

Les cartes de débit, de crédit ou prépayées (y compris les cartes de magasin) ajoutées s'affichent dans une liste de cartes d'Assistant réglages sur les appareils connectés au même compte iCloud. Ces cartes demeurent sur la liste tant qu'elles sont actives sur au moins un appareil. Elles sont supprimées une fois retirées de tous les appareils depuis sept jours. Cette fonctionnalité requiert que l'authentification à deux facteurs soit activée sur le compte iCloud correspondant.

Ajout de cartes de paiement à Apple Pay

Ajout manuel de cartes de paiement

Lors de l'ajout manuel d'une carte, le nom du détenteur, le numéro de carte, la date d'expiration et le code CVV sont utilisés pour faciliter le processus de transfert. L'utilisateur peut entrer ces informations manuellement à partir des Réglages, de l'app Wallet ou de l'app Watch, ou à l'aide de la caméra de l'appareil. Lorsque la caméra capte les informations de la carte, Apple tente de remplir les champs du nom du détenteur, du numéro de carte et de la date d'expiration. La photo n'est jamais enregistrée sur l'appareil ni stockée dans la photothèque. Une fois tous les champs remplis, le processus de vérification de carte vérifie les champs hormis le code CVV. Les données sont ensuite chiffrées puis envoyées au serveur Apple Pay.

Si le processus de vérification de carte renvoie un identifiant de modalités, Apple télécharge les modalités de l'émetteur de la carte et les présente à l'utilisateur. Si ce dernier accepte les modalités, Apple envoie l'identifiant des modalités acceptées et le code CVV au processus de liaison et transfert. En outre, dans le cadre du processus de liaison et transfert, Apple partage des informations de l'appareil avec l'émetteur de la carte ou le réseau de paiement, comme des informations sur l'activité des comptes iTunes et App Store de l'utilisateur (par exemple s'il effectue souvent des transactions dans iTunes), des renseignements sur son appareil (par exemple le numéro de téléphone, le nom et le modèle de l'appareil en question et de tout appareil Apple complémentaire nécessaire à la configuration d'Apple Pay) et sa position approximative au moment de l'ajout de la carte (si le service de localisation est activé). À l'aide de ces informations, l'émetteur de la carte décide d'approuver ou non l'ajout de la carte à Apple Pay.

À l'issue du processus de liaison et transfert, deux opérations ont lieu :

- L'appareil commence à télécharger le fichier de carte Wallet représentant la carte de paiement.

- L’appareil commence à associer la carte au Secure Element.

Le fichier de carte contient des URL permettant de télécharger les illustrations de carte ainsi que les métadonnées de carte telles que les coordonnées, l’app associée de l’émetteur de la carte et les fonctionnalités prises en charge. Il contient également l’état de la carte, qui comprend des informations indiquant par exemple si la personnalisation du Secure Element est terminée, si la carte est actuellement suspendue par l’émetteur ou si une vérification supplémentaire est nécessaire pour que la carte puisse servir à effectuer des paiements avec Apple Pay.

Ajout de cartes de paiement à partir d’un compte iTunes Store

Pour les cartes de paiement dans iTunes, l’utilisateur est parfois invité à saisir à nouveau le mot de passe de son identifiant Apple. Le numéro de carte est obtenu via iTunes, et le processus de vérification de carte est lancé. Si la carte est admissible pour Apple Pay, l’appareil télécharge et affiche les modalités d’utilisation, puis les envoie avec l’identifiant des modalités et le code de sécurité de la carte au processus de liaison et de transfert. Une vérification supplémentaire peut être effectuée pour les cartes liées à un compte iTunes.

Ajout d’une carte de paiement à partir de l’app d’un émetteur de cartes

Lorsqu’une app est inscrite pour être exploitée avec Apple Pay, des clés sont établies pour celle-ci et le serveur de l’émetteur de la carte. Ces clés servent à chiffrer les informations de la carte qui sont envoyées à l’émetteur de celle-ci, ce qui vise à empêcher l’appareil Apple de lire ces informations. Le flux de transfert ressemble à celui de l’ajout de cartes manuel, décrit ci-dessus, sauf que des mots de passe à usage unique sont utilisés au lieu des codes CVV.

Ajout de vérifications supplémentaires

L’émetteur de la carte peut décider si une carte nécessite une vérification supplémentaire. En fonction des services offerts par l’émetteur de la carte, l’utilisateur peut choisir entre différentes options de vérification supplémentaires, telles qu’un message texte, un courriel, un appel au service à la clientèle ou une procédure intégrée à une app tierce approuvée. Pour la vérification par message texte ou par courrier électronique, l’utilisateur choisit une adresse ou un numéro dans les coordonnées figurant dans les dossiers de l’émetteur. Un code à saisir dans l’app Wallet, Réglages ou dans l’app Watch est alors envoyé. Pour le service à la clientèle ou la vérification à l’aide d’une app, l’émetteur doit effectuer son propre processus de communication.

Autorisation de paiement avec Apple Pay

Sur les appareils dotés du Secure Enclave, les paiements sont possibles uniquement après avoir reçu son autorisation. Sur iPhone ou iPad, cela suppose que l’utilisateur s’identifie avec Touch ID, Face ID ou le code de l’appareil. Touch ID ou Face ID, si disponible, constitue la méthode par défaut, mais il est possible d’utiliser le code à tout moment. La vérification par code est automatiquement proposée après trois tentatives infructueuses de reconnaissance d’empreinte digitale ou deux tentatives infructueuses de correspondance faciale et exigée après la cinquième tentative infructueuse. Un code est également exigé si la fonctionnalité Touch ID ou Face ID n’est pas configurée ou n’a pas été activée pour Apple Pay. Pour effectuer un paiement avec une Apple Watch, la montre doit être déverrouillée à l’aide du code, et un double-clic sur le bouton latéral est nécessaire.

Utilisation d’une clé de jumelage partagée

La communication entre le Secure Enclave et le Secure Element est effectuée par l’entremise d’une interface série, le Secure Element étant connecté au contrôleur CCP, lui-même connecté au processeur d’application. Même s’ils ne sont pas directement connectés, le Secure Enclave et le Secure Element peuvent communiquer de manière sécurisée à l’aide d’une clé de jumelage partagée fournie durant le processus de fabrication. Le chiffrement et l’authentification de la communication reposent sur l’algorithme AES, et des nonces cryptographiques sont utilisés de part et d’autre pour assurer une protection contre les attaques par rejeu. La clé de jumelage est générée à l’intérieur du Secure Enclave, à partir de sa clé d’identification et de l’identifiant unique du Secure Element. Cette clé de jumelage est ensuite transférée en toute sécurité du Secure Enclave à un module de sécurité matériel (HSM, Hardware Security Module) en usine, qui dispose du matériel nécessaire pour ensuite injecter la clé de jumelage dans le Secure Element.

Autorisation des transactions sécurisées

Lorsque l’utilisateur autorise une transaction, ce qui comprend un geste communiqué directement au Secure Enclave, ce dernier envoie au Secure Element des données signées relatives au type d’authentification ainsi que des détails concernant le type de transaction (sans contact ou au sein d’apps), le tout lié à une valeur d’autorisation aléatoire (AR, Authorization Random). La valeur AR est générée dans le Secure Enclave lorsqu’un utilisateur transfère pour la première fois une carte de crédit et est conservée tant qu’Apple Pay est activé. Elle est protégée par le chiffrement et le mécanisme de protection contre les attaques par retour en arrière du Secure Enclave. Elle est transmise en toute sécurité au Secure Element au moyen de la clé de jumelage. À la réception d’une nouvelle valeur AR, le Secure Element marque toutes les cartes précédemment ajoutées comme supprimées.

Utilisation d’un cryptogramme de paiement à des fins de sécurité dynamique

Les transactions de paiement provenant d’applets de paiement comprennent un cryptogramme de paiement ainsi qu’un numéro de compte de l’appareil. Ce cryptogramme, un code unique, est calculé à l’aide d’un compteur de transactions et d’une clé. Ce compteur est incrémenté pour chaque nouvelle transaction. La clé est fournie dans l’applet de paiement pendant la personnalisation et connue du réseau de paiement ou de l’émetteur de la carte. En fonction du système de paiement, il est possible d’utiliser d’autres données pour les calculs, y compris :

- Un numéro imprévisible de terminal destiné aux transactions CCP (communication en champ proche)
- Un nonce généré par le serveur Apple Pay, pour les transactions effectuées dans une app

Ces codes de sécurité sont fournis au réseau de paiement et à l’émetteur de la carte, permettant à ce dernier de vérifier chaque transaction. La longueur des codes de sécurité peut varier en fonction du type de transaction.

Paiements par carte avec Apple Pay

Paiement par carte en magasin

Lorsque l'iPhone ou l'Apple Watch est activé et qu'il détecte un champ CCP, il présente à l'utilisateur la carte demandée (si la sélection automatique est activée pour cette carte) ou la carte par défaut, qui est gérée dans Réglages. L'utilisateur peut également accéder à l'app Wallet et choisir une carte ou, si l'appareil est verrouillé :

- appuyer deux fois sur le bouton principal des appareils dotés de Touch ID;
- appuyer deux fois sur le bouton latéral des appareils dotés de Face ID.

L'utilisateur doit ensuite s'identifier avec Touch ID, Face ID ou son code pour que les données de paiement soient transmises. Quand l'Apple Watch est déverrouillée, appuyer deux fois sur le bouton latéral permet d'activer la carte par défaut pour le paiement. Aucune donnée de paiement ne peut être envoyée sans authentification de l'utilisateur.

Une fois que l'utilisateur a été authentifié, le numéro de compte de l'appareil et un code de sécurité dynamique propre à la transaction sont utilisés pour traiter le paiement. Ni Apple ni l'appareil de l'utilisateur n'envoient les numéros complets des cartes de paiement aux vendeurs. Apple peut recevoir des données de transaction anonymes, telles que l'heure et le lieu approximatifs de la transaction, destinées à améliorer Apple Pay et d'autres produits et services d'Apple.

Paiement par carte dans les apps

Apple Pay peut également être utilisé pour effectuer des paiements dans les apps pour iPhone, iPad, Mac et Apple Watch. Lorsqu'un utilisateur paie dans une app avec Apple Pay, Apple reçoit les données de transaction chiffrées. Avant l'envoi de ces données au développeur ou au vendeur, Apple chiffre de nouveau la transaction à l'aide d'une clé propre au développeur. Apple Pay conserve des données de transaction anonymes, comme le montant approximatif de l'achat. Ces données ne peuvent être associées à un utilisateur précis et n'incluent aucune information sur le contenu des achats.

Lorsqu'une app lance une transaction de paiement Apple Pay, les serveurs Apple Pay reçoivent la transaction chiffrée de l'appareil avant le vendeur. Puis, ils chiffrent à nouveau la transaction au moyen d'une clé propre au vendeur avant de la transmettre à ce dernier.

Lorsqu'une app demande un paiement, elle appelle une API pour déterminer si l'appareil prend en charge Apple Pay et si l'utilisateur possède des cartes de paiement capables d'effectuer des paiements sur les réseaux de paiement acceptés par le vendeur. L'app demande les renseignements dont elle a besoin pour traiter et terminer la transaction (coordonnées et adresses d'expédition et de facturation, par exemple). L'app demande ensuite à iOS, à iPadOS ou à watchOS de présenter le formulaire Apple Pay, qui demande des informations pour le compte de l'app ainsi que d'autres renseignements nécessaires, par exemple la carte à utiliser.

L'app reçoit alors les informations relatives à la ville, à la province et au code postal nécessaires pour calculer les frais d'expédition. L'ensemble des informations demandées n'est transmis à l'app que lorsque l'utilisateur a autorisé le paiement avec Touch ID, Face ID ou le code de l'appareil. Une fois le paiement autorisé, les informations figurant sur le formulaire Apple Pay sont envoyées au vendeur.

Autorisation de paiement par l'app

Lorsque l'utilisateur autorise le paiement, un appel est effectué auprès des serveurs Apple Pay en vue d'obtenir un nonce cryptographique similaire à la valeur renvoyée par le terminal CCP utilisé pour les transactions en magasin. Le nonce ainsi que d'autres données de transaction sont transmis au Secure Element afin de générer une accréditation de paiement destinée à être chiffrée à l'aide d'une clé Apple. Une fois l'accréditation de paiement chiffrée générée par le Secure Element, elle est transmise aux serveurs Apple Pay, qui la déchiffrent, comparent le nonce inclus dans l'accréditation au nonce envoyé par les serveurs Apple Pay, puis effectuent un nouveau chiffrement de cette accréditation de paiement à l'aide de la clé de vendeur associée à l'identifiant du vendeur. Le paiement est ensuite renvoyé à l'appareil, qui le remet à l'app par l'intermédiaire de l'API. L'app la transfère alors au système du vendeur en vue de son traitement. Le vendeur peut ainsi déchiffrer l'accréditation de paiement à l'aide de sa clé privée afin de la traiter. Grâce à ces informations et à la signature provenant des serveurs d'Apple, le vendeur peut vérifier que la transaction lui était bien destinée.

Les API requièrent une déclaration d'autorisation spécifiant les identifiants de vendeur pris en charge. Une app peut également inclure des données supplémentaires (comme un numéro de commande ou l'identité du client) à envoyer au Secure Element pour les faire signer afin que la transaction ne puisse pas être détournée vers un autre client. Cette tâche est effectuée par le développeur de l'app, qui peut préciser les données d'application (applicationData) de la demande de paiement (PKPaymentRequest). Un hachage de ces données est inclus dans les données de paiement chiffrées. Le vendeur doit ensuite vérifier que le hachage applicationData correspond à ce qui se trouve dans les données de paiement.

Paiement par carte sur les sites Web

Apple Pay peut être utilisé pour effectuer des paiements sur les sites Web avec un iPhone, un iPad, une Apple Watch ou un ordinateur Mac équipé de Touch ID. Les transactions Apple Pay peuvent également être commencées sur un Mac et terminées sur un iPhone ou une Apple Watch sur lesquels Apple Pay est activé avec le même compte iCloud.

L'utilisation d'Apple Pay en ligne requiert que tous les sites Web participants soient enregistrés auprès d'Apple. La validation du nom de domaine est effectuée une fois que le domaine est enregistré et qu'un certificat de client TLS est émis par Apple. Les sites Web qui prennent en charge Apple Pay doivent fournir leur contenu par HTTPS. Pour chaque transaction de paiement, les sites Web doivent obtenir une session de vendeur sécurisée et unique sur un serveur Apple à l'aide du certificat client TLS émis par Apple. Les données de session de vendeur sont signées par Apple. Une fois une signature de session de vendeur vérifiée, un site Web peut demander si l'utilisateur dispose d'un appareil prenant en charge Apple Pay et si une carte de crédit, de débit ou prépayée est activée sur l'appareil. Aucun autre renseignement n'est partagé. Si l'utilisateur ne veut pas partager ces informations, il peut désactiver les requêtes Apple Pay dans les réglages de confidentialité de Safari de son iPhone, de son iPad ou de son Mac.

Une fois qu'une session de vendeur est validée, les mesures de sécurité et de confidentialité sont les mêmes que lorsqu'un utilisateur effectue un paiement dans une app.

Si l'utilisateur transmet des données de paiement d'un Mac à un iPhone ou à une Apple Watch, la transmission Handoff d'Apple Pay utilise le protocole du service d'identité d'Apple (IDS) chiffré de bout en bout pour transmettre ces données entre le Mac de l'utilisateur et l'appareil d'autorisation. Le protocole IDS utilise les clés d'appareil de l'utilisateur pour effectuer le chiffrement, de sorte qu'aucun autre appareil ne puisse déchiffrer ces informations. Apple n'a pas accès à ces clés. Pour chaque transmission Handoff, Apple Pay doit obtenir de l'appareil certains renseignements sur la carte de crédit de l'utilisateur, notamment le type, l'identifiant unique et certaines métadonnées. Le numéro de compte de l'appareil associé à la carte de l'utilisateur n'est pas partagé et demeure stocké de façon sécurisée sur l'iPhone ou l'Apple Watch. Apple transfère également en toute sécurité les coordonnées et adresses d'expédition et de facturation de l'utilisateur récemment utilisées au moyen du trousseau iCloud.

Une fois que l'utilisateur autorise le paiement à l'aide de Touch ID, de Face ID, de son code ou en appuyant deux fois sur le bouton latéral de son Apple Watch, un jeton de paiement unique et chiffré pour chaque certificat de site Web de vendeur est transmis de façon sécurisée de l'iPhone ou de l'Apple Watch au Mac de l'utilisateur, puis est transmis au site Web du vendeur.

Seuls les appareils à proximité les uns des autres peuvent demander et effectuer un paiement. La proximité est déterminée au moyen de notifications Bluetooth faible énergie (BLE).

Cartes sans contact dans Apple Pay

Pour transmettre des données de cartes prises en charge vers des terminaux CCP compatibles, Apple utilise le protocole de services à valeur ajoutée (SVA) d'Apple. Le protocole de SVA peut être implémenté sur les terminaux sans contact et exploite la technologie CCP pour communiquer avec les appareils Apple pris en charge. Le protocole de SVA fonctionne sur une courte distance et peut être utilisé pour présenter séparément des cartes sans contact ou effectuer une transaction Apple Pay.

Lorsque l'appareil est tenu près du terminal CCP, ce dernier engage la réception des informations sur la carte en envoyant une demande de carte. Si l'utilisateur possède une carte avec l'identifiant du fournisseur de carte, il doit autoriser son utilisation à l'aide de Touch ID, de Face ID ou de son code. Les informations sur la carte, les données d'horodatage et une clé ECDH P-256 aléatoire à usage unique sont utilisées conjointement avec la clé publique du fournisseur de carte pour calculer une clé de chiffrement pour les données de la carte, lesquelles sont envoyées au terminal.

Sous iOS 12 à iOS 13, les utilisateurs peuvent sélectionner manuellement une carte avant de la présenter au terminal CCP du vendeur. Sous iOS 13.1 et les versions ultérieures, les fournisseurs de cartes peuvent configurer manuellement les cartes sélectionnées pour qu'elles exigent ou non l'authentification de l'utilisateur.

Invalidation des cartes avec Apple Pay

Les cartes de crédit, de débit et prépayées ajoutées au Secure Element ne peuvent être utilisées que si une autorisation est présentée au Secure Element au moyen de la clé de jumelage et de la valeur d'autorisation aléatoire (AR, Authorization Random) utilisées lors de l'ajout de la carte. À la réception d'une nouvelle valeur AR, le Secure Element marque toutes les cartes précédemment ajoutées comme supprimées. Cela permet au système d'exploitation d'ordonner au Secure Enclave de rendre des cartes inutilisables en marquant la copie de la valeur AR en sa possession comme invalide dans les situations suivantes :

Méthode	Appareil
Le code est désactivé.	iPhone, iPad, Apple Watch
Le mot de passe est désactivé.	Mac
L'utilisateur se déconnecte d'iCloud.	iPhone, iPad, Mac, Apple Watch
L'utilisateur sélectionne Effacer contenu et réglages.	iPhone, iPad, Apple Watch
L'appareil est restauré à partir du mode de récupération.	iPhone, iPad, Mac, Apple Watch
Le jumelage est désactivé.	Apple Watch

Suspension, retrait et suppression de cartes

Les utilisateurs ont la possibilité de suspendre Apple Pay sur leur iPhone, iPad ou Apple Watch en plaçant l'appareil en mode Perdu à l'aide de la fonction Localiser. Ils peuvent également retirer et supprimer leurs cartes d'Apple Pay au moyen de l'app Localiser, sur iCloud.com ou directement sur leur appareil à l'aide de l'app Wallet. Les cartes enregistrées dans une Apple Watch peuvent être supprimées à l'aide des réglages iCloud, dans l'app Watch sur iPhone ou directement sur la montre. L'émetteur de la carte ou le réseau de paiement correspondant suspend ou supprime alors la possibilité d'effectuer des paiements avec la carte avec Apple Pay sur l'appareil, même si celui-ci est hors ligne et n'est pas connecté à un réseau cellulaire ou Wi-Fi. Les utilisateurs peuvent également appeler l'émetteur de la carte pour suspendre ou retirer des cartes d'Apple Pay.

Lorsqu'un utilisateur efface l'intégralité du contenu de son appareil en choisissant l'option Effacer contenu et réglages, en employant l'app Localiser ou en restaurant son appareil, l'iPhone, l'iPad, l'iPod touch, le Mac et l'Apple Watch demandent au Secure Element de marquer toutes les cartes comme supprimées. Cette opération rend dès lors toutes les cartes inutilisables jusqu'à ce que les serveurs Apple Pay puissent être contactés afin de supprimer complètement les cartes dans le Secure Element. Parallèlement, le Secure Enclave marque la valeur AR comme étant invalide, de sorte qu'il ne soit plus possible d'autoriser des paiements avec des cartes précédemment enregistrées. Une fois en ligne, l'appareil essaie de contacter les serveurs Apple Pay pour veiller à ce que toutes les cartes présentes dans le Secure Element soient effacées.

Sécurité d’Apple Cash sous iOS, iPadOS et watchOS

Aperçu

Sous iOS 11.2 ou version ultérieure, iPadOS13.1 ou version ultérieure, ou watchOS 4.2 ou version ultérieure, Apple Pay peut être utilisé sur iPhone, iPad ou Apple Watch pour envoyer de l’argent à d’autres utilisateurs, leur en demander ou en recevoir. Lorsqu’un utilisateur reçoit de l’argent, la somme est créditée sur un compte Apple Cash accessible dans l’app Wallet ou dans Réglages > Wallet et Apple Pay sur n’importe quel appareil admissible sur lequel l’utilisateur s’est connecté avec son identifiant Apple.

Dans iOS 14, iPadOS 14 et watchOS 7, l’organisateur d’une famille iCloud qui a validé son identité peut activer Apple Cash pour les membres de sa famille âgés de moins de 18 ans. Facultativement, l’organisateur peut restreindre les possibilités d’envoi de fonds de ces utilisateurs aux membres de la famille ou aux contacts uniquement. Si le membre de la famille âgé de moins de 18 ans effectue une récupération du compte de son identifiant Apple, l’organisateur de la famille doit réactiver manuellement la carte Apple Cash de cet utilisateur. Si le membre de la famille âgé de moins de 18 ans ne fait plus partie de la famille iCloud, son solde Apple Cash est automatiquement transféré au compte de l’organisateur.

Lorsque l’utilisateur configure Apple Cash, des informations similaires à celles qu’il partage lorsqu’il ajoute une carte de paiement pourraient être partagées avec notre banque partenaire, Green Dot Bank, et Apple Payments Inc., une filiale en propriété exclusive d’Apple créée pour stocker et traiter l’information d’une manière indépendante et inconnue du reste d’Apple et ainsi protéger les données confidentielles de l’utilisateur. Ces renseignements sont utilisés uniquement à des fins réglementaires, de dépannage et de prévention de la fraude.

Utiliser Apple Cash dans iMessage

Pour utiliser les paiements de personne à personne et Apple Cash, un utilisateur doit être connecté à son compte iCloud sur un appareil compatible avec Apple Cash et y avoir configuré l’authentification à deux facteurs. Les demandes et les transferts d’argent entre utilisateurs sont engagés à partir de l’app Messages ou par l’intermédiaire de Siri. Lorsqu’un utilisateur tente d’envoyer de l’argent, iMessage affiche le formulaire Apple Pay. Le solde Apple Cash est toujours utilisé en premier. Au besoin, des fonds supplémentaires sont débités d’une carte de paiement que l’utilisateur a ajoutée à l’app Wallet.

Utilisation d’Apple Cash en magasin, dans les apps et sur le Web

La carte Apple Cash dans l’app Wallet peut être utilisée avec Apple Pay pour effectuer des paiements en magasin, dans les apps ou sur le Web. L’argent du compte Apple Cash peut également être transféré vers un compte bancaire. En plus de recevoir de l’argent de la part d’un autre utilisateur, il est possible d’ajouter de l’argent à un compte Apple Cash à partir d’une carte de débit ou d’une carte prépayée dans l’app Wallet.

Apple Payments Inc. stocke les données de transaction de l’utilisateur et peut les utiliser à des fins réglementaires, de dépannage ou de prévention de la fraude une fois une transaction terminée. Le reste d’Apple ne sait pas à qui l’utilisateur envoie de l’argent, de qui il en reçoit, ni les endroits où il effectue des achats avec sa carte Apple Cash.

Lorsque l'utilisateur envoie de l'argent avec Apple Pay, en ajoute à un compte Apple Cash ou en transfère vers un compte bancaire, un contact est établi avec les serveurs Apple Pay afin d'obtenir un nonce cryptographique, similaire à la valeur renvoyée pour Apple Pay dans les apps. Le nonce ainsi que d'autres données de transaction sont transmis au Secure Element pour générer une signature de paiement. Lorsque la signature de paiement sort du Secure Element, elle est relayée aux serveurs Apple Pay. L'authenticité, l'intégrité et l'exactitude de la transaction sont vérifiées par les serveurs Apple Pay à l'aide de la signature de paiement et du nonce. Le transfert d'argent est ensuite engagé, et l'utilisateur est avisé de la réussite de la transaction.

Si la transaction implique :

- Une carte de débit pour ajouter des fonds à Apple Cash
- L'ajout de fonds supplémentaires si le solde Apple Cash est insuffisant

Les informations d'identification de paiement chiffrées sont également produites et envoyées aux serveurs Apple Pay, d'une façon semblable au fonctionnement d'Apple Pay dans les apps et sur les sites Web.

Si le solde Apple Cash excède un certain montant ou qu'une activité inhabituelle est détectée, l'utilisateur est invité à valider son identité. Les informations que l'utilisateur fournit pour valider son identité, comme son numéro d'assurance sociale ou des réponses à des questions (par exemple le nom de la rue d'une adresse antérieure), sont transmises en toute sécurité au partenaire d'Apple et chiffrées à l'aide de sa clé. Apple n'est pas en mesure de déchiffrer ces données. L'utilisateur sera invité à revalider son identité s'il effectue une récupération du compte de son identifiant Apple avant de pouvoir disposer à nouveau de l'accès à son solde Apple Cash.

Sécurité d'Apple Card

Demande d'Apple Card dans l'app Wallet

Sous iOS 12.4, macOS 10.14.6, watchOS 5.3 et les versions ultérieures de ces systèmes d'exploitation, l'Apple Card peut être utilisée avec Apple Pay pour effectuer des paiements en magasin, dans les apps et sur le Web.

Pour présenter une demande d'Apple Card, l'utilisateur doit être connecté à son compte iCloud sur un appareil iOS ou iPadOS compatible avec Apple Pay et y avoir configuré l'authentification à deux facteurs. Lorsque la demande est approuvée, l'Apple Card est disponible dans l'app Wallet ou dans Réglages > Wallet et Apple Pay sur n'importe quel appareil admissible sur lequel l'utilisateur s'est connecté avec son identifiant Apple.

Lorsqu'un utilisateur demande une Apple Card, les informations d'identification de l'utilisateur sont vérifiées de façon sécurisée par les partenaires fournisseurs d'identité d'Apple, puis partagées avec Goldman Sachs Bank USA pour valider l'identité et évaluer la solvabilité.

Des informations, telles que le numéro d'assurance sociale ou la photo de la pièce d'identité fournis dans le cadre de la demande, sont transmises de façon sécurisée aux partenaires fournisseurs d'identité d'Apple ou à Goldman Sachs Bank USA, chiffrées à l'aide de leurs clés respectives. Apple n'est pas en mesure de déchiffrer ces données.

Les renseignements sur le revenu fournis dans le cadre de la demande et ceux sur le compte bancaire utilisé pour payer les factures sont transmis de façon sécurisée à Goldman Sachs Bank USA, chiffrés à l'aide de sa clé. Les renseignements sur le compte bancaire sont enregistrés dans le trousseau. Apple n'est pas en mesure de déchiffrer ces données.

Lors de l'ajout de l'Apple Card à l'app Wallet, les mêmes informations que celles demandées pour l'ajout d'une carte de paiement peuvent être partagées avec la banque partenaire d'Apple, Goldman Sachs Bank USA, et Apple Payments Inc. Ces renseignements sont utilisés uniquement à des fins réglementaires, de dépannage et de prévention de la fraude.

Il est possible de commander une carte physique à partir de l'Apple Card dans l'app Wallet. Une fois que l'utilisateur a reçu la carte physique, celle-ci est activée à l'aide de l'étiquette CCP présente dans l'enveloppe à deux volets. L'étiquette est unique pour chaque carte et ne peut pas être utilisée pour activer la carte d'un autre utilisateur. La carte peut aussi être activée manuellement dans les réglages de Wallet. De plus, l'utilisateur peut également choisir de verrouiller ou de déverrouiller la carte physique à tout moment dans l'app Wallet.

Paiements avec l'Apple Card et renseignements sur la carte Apple Wallet

Les paiements dus sur le compte de l'Apple Card peuvent être effectués à partir de l'app Wallet sous iOS avec Apple Cash et un compte bancaire. Il est possible de programmer des paiements de facture récurrents ou ponctuels à une date précise avec Apple Cash et un compte bancaire. Lorsqu'un utilisateur effectue un paiement, les serveurs Apple Pay sont appelés pour obtenir un nonce cryptographique, un peu comme pour Apple Cash. Le nonce, accompagné des données de paiement, est envoyé au Secure Element pour générer une signature. Lorsque la signature de paiement sort du Secure Element, elle est relayée aux serveurs Apple Pay. L'authenticité, l'intégrité et l'exactitude du paiement sont vérifiées à l'aide de la signature et du nonce par les serveurs Apple Pay. La commande est ensuite transmise à Goldman Sachs Bank USA aux fins de traitement.

L'affichage du numéro de l'Apple Card dans l'app Wallet requiert l'authentification de l'utilisateur avec Face ID, Touch ID ou un code. L'utilisateur peut le remplacer dans la section des informations sur la carte, ce qui désactive l'ancien numéro.

Ajout de cartes de transport et de cartes étudiantes à Wallet

Cartes de transport

Dans plusieurs marchés du monde, les utilisateurs peuvent ajouter les cartes de transport compatibles dans l'app Wallet sur les modèles d'iPhone et d'Apple Watch prenant en charge cette fonctionnalité. Selon l'exploitant du service de transport en commun, on peut faire cet ajout soit en transférant la valeur et le titre de transport d'une carte physique vers sa représentation numérique Apple Wallet, soit en transférant une nouvelle carte de transport dans l'app Wallet à partir de l'app de l'émetteur de cette carte. Une fois les cartes de transport ajoutées à l'app Wallet, les utilisateurs peuvent utiliser le transport en commun simplement en tenant leur iPhone ou leur Apple Watch près du lecteur. Certaines cartes peuvent également être utilisées pour faire des paiements.

Les cartes de transport ajoutées sont associées au compte iCloud d'un utilisateur. Si l'utilisateur ajoute plus d'une carte à l'app Wallet, Apple ou l'émetteur de la carte de transport peut être en mesure de lier les informations personnelles de l'utilisateur et les informations de compte associées aux cartes. Les cartes de transport et leurs transactions sont protégées par un ensemble de clés cryptographiques hiérarchiques.

Pendant le processus de transfert du solde d'une carte physique vers l'app Wallet, les utilisateurs sont invités à saisir certaines informations spécifiques. Les utilisateurs peuvent également devoir fournir des renseignements personnels pour prouver qu'ils ont la carte en main. Lors du transfert des cartes d'un iPhone vers une Apple Watch, les deux appareils doivent être en ligne.

Il est possible d'ajouter des fonds à partir de cartes de crédit, de débit ou prépayées dans Wallet ou l'app de l'émetteur de la carte de transport. Pour comprendre la sécurité relative à l'ajout de fonds lors de l'utilisation d'Apple Pay, consultez la section Paiement par carte dans les apps. Pour apprendre comment la carte de transport est transférée à partir de l'app de son émetteur, consultez la section Ajout d'une carte de paiement à partir de l'app d'un émetteur de cartes.

Lorsque le transfert d'une carte physique est pris en charge, l'émetteur de la carte de transport détient les clés cryptographiques nécessaires pour authentifier la carte physique et vérifier les données saisies par l'utilisateur. Après la vérification des données, le système peut créer un numéro de compte de l'appareil pour le Secure Element et activer la nouvelle carte dans l'app Wallet avec le solde transféré. Dans certaines villes, la carte physique est désactivée après son transfert.

Au terme de ces méthodes de transfert, si le solde de la carte de transport est stocké sur l'appareil, il est chiffré dans un applet désigné dans le Secure Element. L'exploitant du service de transport en commun détient les clés pour effectuer les opérations cryptographiques sur les données de la carte dans le cadre de transactions liées au solde.

Par défaut, les utilisateurs bénéficient du service simplifié Transport express qui leur permet de prendre le transport en commun sans utiliser Touch ID, Face ID ou leur code. Les informations comme les stations récemment visitées, l'historique des transactions et les billets supplémentaires sont accessibles par les lecteurs de carte sans contact à proximité si le mode Express est activé. Les utilisateurs peuvent exiger l'utilisation de Touch ID, de Face ID ou du code en désactivant Transport express dans les réglages Wallet et Apple Pay.

Comme c'est le cas pour les autres cartes Apple Pay, les utilisateurs peuvent suspendre ou supprimer les cartes de transport en :

- effaçant les données de l'appareil à distance avec Localiser;
- activant le mode Perdu avec Localiser;
- saisissant une commande d'effacement à distance par une solution de gestion des appareils mobiles (GAM);
- supprimant toutes les cartes figurant sur la page du compte de leur identifiant Apple;
- supprimant toutes les cartes à partir d'iCloud.com;
- supprimant toutes les cartes de l'app Wallet;
- supprimant la carte de l'app de l'émetteur.

Les serveurs Apple Pay avisent alors l'exploitant du service de transport en commun de suspendre ou de désactiver ces cartes. Si un utilisateur supprime une carte de transport d'un appareil en ligne, le solde est récupérable en rajoutant la carte à un appareil connecté avec le même identifiant Apple. Si un appareil est hors ligne, éteint ou inutilisable, la récupération peut ne pas être possible.

Cartes de crédit et de débit

Dans certaines villes, les lecteurs de cartes de transport permettent aux usagers de payer leurs trajets au moyen de cartes (intelligentes) EMV. Lorsque les usagers présentent une carte de crédit ou de débit EMV à ces lecteurs, l'authentification de l'utilisateur est requise, tout comme lorsque l'utilisateur effectue un achat en magasin avec une carte de crédit ou de débit.

Sous iOS 12.3 et les versions ultérieures, certaines cartes de paiement EMV dans l'app Wallet peuvent être activées pour le transport express, ce qui permet à l'utilisateur de payer pour un trajet auprès des exploitants de services de transport en commun pris en charge sans Touch ID, Face ID ou un code. Lorsqu'un utilisateur transfère des cartes de paiement EMV, la première ajoutée à l'app Wallet est activée pour le transport express. L'utilisateur peut toucher le bouton Plus sur le devant de la carte dans l'app Wallet et désactiver le transport express sur cette carte en sélectionnant Aucune dans les réglages. L'utilisateur peut aussi sélectionner une autre carte de paiement comme carte de transport express dans l'app Wallet. Touch ID, Face ID ou le code est requis pour réactiver le transport express ou sélectionner une autre carte de transport express.

Apple Card et Apple Cash sont compatibles avec le mode Express.

Cartes étudiantes

Sous iOS 12 et les versions ultérieures, les étudiants, les professeurs et les employés des établissements d'enseignement participants peuvent ajouter leur carte étudiante à l'app Wallet sur les modèles d'iPhone et d'Apple Watch prenant en charge cette fonctionnalité et s'en servir pour accéder à certains lieux et payer partout où leur carte est acceptée.

L'utilisateur ajoute sa carte étudiante à l'app Wallet à partir d'une app fournie par l'émetteur de la carte ou l'établissement participant. Le processus technique est le même que celui décrit dans la section Ajout de cartes de paiement à partir de l'app d'un émetteur de cartes. Par ailleurs, les apps émettrices doivent prendre en charge l'authentification à deux facteurs sur les comptes qui protègent l'accès à leurs cartes étudiantes. Une carte peut être configurée en même temps sur un maximum de deux appareils Apple compatibles connectés avec le même identifiant Apple.

Lorsqu'une carte étudiante est ajoutée à l'app Wallet, le mode Express est activé par défaut. Les cartes étudiantes en mode Express interagissent avec les terminaux compatibles sans Touch ID, Face ID, authentification par code ni double-clic du bouton latéral de l'Apple Watch. L'utilisateur peut toucher le bouton Plus sur le devant de la carte dans l'app Wallet et désactiver le mode Express. Touch ID, Face ID ou le code est requis pour réactiver le mode Express.

Les cartes étudiantes peuvent être désactivées ou supprimées en :

- effaçant les données de l'appareil à distance avec Localiser;
- activant le mode Perdu avec Localiser;

- recevant une commande d’effacement à distance par une solution de gestion des appareils mobiles (GAM);
- supprimant toutes les cartes figurant sur la page du compte de leur identifiant Apple;
- supprimant toutes les cartes à partir d’iCloud.com;
- supprimant toutes les cartes de l’app Wallet;
- supprimant la carte de l’app de l’émetteur.

iMessage

Aperçu de la sécurité d’iMessage

Conçu par Apple, iMessage est un service de messagerie pour appareils iOS et iPadOS, Apple Watch et ordinateurs Mac. iMessage prend en charge aussi bien le texte que les pièces jointes, telles que les photos, les contacts, les lieux et les liens, directement dans un message (par exemple une icône de pouce vers le haut). Les messages s’affichent sur tous les appareils enregistrés d’un utilisateur, de sorte qu’une conversation entamée sur un appareil puisse être poursuivie sur n’importe quel autre appareil. iMessage fait largement appel au service de notifications Push d’Apple (APN). Apple ne conserve pas le contenu des messages ni des pièces jointes, qui est protégé par un système de chiffrement de bout en bout, afin que personne d’autre que l’expéditeur et le destinataire ne puisse y accéder. Apple n’est pas en mesure de déchiffrer ces données.

Lorsqu’un utilisateur active iMessage sur un appareil, des paires de clés de chiffrement et de signature à utiliser avec le service sont générées. Pour le chiffrement, il s’agit d’une clé RSA 1 280 bits et d’une clé EC 256 bits sur la courbe NIST P-256. Les clés de signature ECDSA (Elliptic Curve Digital Signature Algorithm, algorithme de signature numérique basé sur les courbes elliptiques) 256 bits sont utilisées pour les signatures. Les clés privées sont enregistrées dans le trousseau de l’appareil et ne sont disponibles qu’après le premier déverrouillage. Les clés publiques sont envoyées au service d’identité d’Apple (IDS), où elles sont associées au numéro de téléphone ou à l’adresse courriel de l’utilisateur, ainsi qu’à l’adresse du service APN de l’appareil.

Au fur et à mesure que les utilisateurs activent d’autres appareils à utiliser avec iMessage, leurs clés de chiffrement et de signature publiques, les adresses de service APN et les numéros de téléphone associés sont ajoutés au service de répertoire. Les utilisateurs ont également la possibilité d’ajouter des adresses électroniques qui sont vérifiées au moyen d’un lien de confirmation. Les numéros de téléphone sont vérifiés par la carte SIM et le réseau de l’opérateur. Pour certains réseaux, il faut utiliser la fonctionnalité SMS (une boîte de dialogue demande la confirmation de l’utilisateur si le SMS n’est pas gratuit). La vérification du numéro de téléphone peut être nécessaire pour plusieurs services du système en plus d’iMessage, comme FaceTime et iCloud. Tous les appareils enregistrés de l’utilisateur affichent un message d’alerte dès qu’une nouvelle adresse électronique, un nouvel appareil ou un nouveau numéro de téléphone est ajouté.

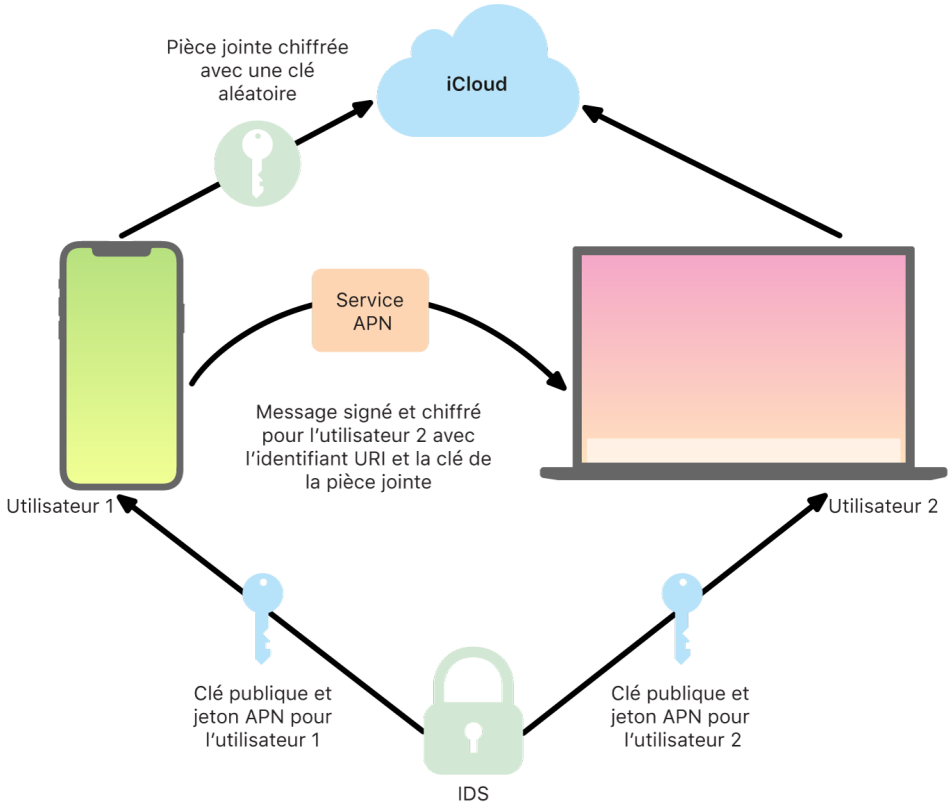
Envoi et réception sécurisés des messages par iMessage

L'utilisateur lance une nouvelle conversation iMessage en saisissant une adresse ou un nom. S'il saisit un numéro de téléphone ou une adresse électronique, l'appareil entre en contact avec le service d'identité d'Apple (IDS) pour récupérer les clés publiques et les adresses de service APN de tous les appareils associés au destinataire. Si l'utilisateur saisit un nom, l'appareil utilise d'abord l'app Contacts de l'utilisateur pour récupérer les numéros de téléphone et les adresses électroniques associés à ce nom, puis récupère les clés publiques et les adresses de service APN à l'aide du service IDS.

Le message sortant envoyé par l'utilisateur est chiffré séparément pour chacun des appareils du destinataire. Les clés de chiffrement et de signature publiques des appareils récepteurs sont récupérées par l'entremise de l'IDS. Pour chaque appareil récepteur, l'appareil émetteur génère une valeur 88 bits aléatoire et l'utilise comme clé HMAC-SHA256 pour construire une valeur 40 bits dérivée de la clé publique et du texte brut de l'expéditeur et du destinataire. La concaténation des valeurs 88 bits et 40 bits crée une clé 128 bits, qui chiffre le message à l'aide de l'algorithme AES en mode CTR (basé sur un compteur). Cette valeur 40 bits est utilisée par le côté récepteur pour vérifier l'intégrité du texte brut déchiffré. Cette clé AES propre à chaque message est chiffrée via RSA-OAEP vers la clé publique de l'appareil récepteur. La combinaison constituée du texte du message chiffré et de la clé de message chiffrée est ensuite hachée avec l'algorithme SHA-1, et le hachage est signé avec l'algorithme ECDSA (Elliptic Curve Digital Signature Algorithm, algorithme de signature numérique basé sur les courbes elliptiques) à l'aide de la clé de signature privée de l'appareil émetteur. Sous iOS 13, iPadOS 13.1 et les versions ultérieures de ces systèmes d'exploitation, les appareils peuvent utiliser un chiffrement ECIES (Elliptic Curve Integrated Encryption Scheme, système de chiffrement intégré basé sur les courbes elliptiques) au lieu d'un chiffrement RSA.

Les messages résultants (un pour chaque appareil récepteur) sont constitués du texte de message chiffré, de la clé de message chiffrée et de la signature numérique de l'expéditeur. Ils sont ensuite transmis au service APN en vue de leur livraison. Les métadonnées, comme les données d'horodatage et les informations de routage du service APN, ne sont pas chiffrées. La communication avec le service APN est chiffrée par l'intermédiaire d'un canal TLS à confidentialité persistante.

Le service APN ne peut relayer que des messages de 4 ko ou 16 ko, selon la version d'iOS ou d'iPadOS. Si le texte du message est trop long ou s'il contient un fichier, comme une photo, la pièce jointe est chiffrée par AES en mode CTR à l'aide d'une clé 256 bits générée aléatoirement, puis est téléchargée vers iCloud. La clé AES destinée à la pièce jointe, son identifiant de ressource uniforme (URI) et un hachage SHA-1 de sa forme chiffrée sont ensuite envoyés au destinataire en tant que contenu de message iMessage, la confidentialité et l'intégrité de ces éléments étant protégées par un chiffrement iMessage normal (voir l'illustration suivante).



Envoi et réception des messages par iMessage.

Dans le cas d'une conversation de groupe, ce processus est répété pour chaque destinataire et ses appareils.

Du côté du destinataire, chaque appareil reçoit sa copie du message via le service APN et, si nécessaire, récupère la pièce jointe sur iCloud. Le numéro de téléphone ou l'adresse électronique de l'expéditeur est comparé aux données figurant dans les contacts du destinataire afin de pouvoir afficher un nom si possible.

Comme pour toutes les notifications de type Push, le message est supprimé du service APN dès sa livraison. Contrairement à d'autres notifications du service APN, les messages iMessage sont placés en file d'attente en attendant d'être livrés à des appareils déconnectés. Les messages sont conservés pendant 30 jours au maximum.

Partage sécurisé du nom et de la photo par iMessage

Le partage du nom et de la photo par iMessage permet à un utilisateur de partager un nom et une photo avec iMessage. L'utilisateur peut sélectionner sa fiche personnelle ou personnaliser le nom et inclure l'image de son choix. Le partage du nom et de la photo par iMessage utilise un système en deux étapes pour distribuer le nom et la photo.

Les données sont sous-divisées en champs, qui sont chiffrés et authentifiés séparément en plus d'être authentifiés ensemble dans le cadre du processus ci-dessous. Il y a trois champs :

- Nom
- Photo
- Nom de fichier photo

La première étape de la création de données consiste à générer de façon aléatoire une clé d'enregistrement 128 bits sur l'appareil. Cette clé est ensuite dérivée à l'aide de la fonction HKDF-HMAC-SHA256 pour créer trois sous-clés : Key 1:Key 2:Key 3 = HKDF(record key, "nicknames"). Pour chaque champ, un vecteur d'initialisation (IV) aléatoire 96 bits est généré, et les données sont chiffrées à l'aide de l'algorithme AES-CTR et de la clé 1. Un code d'authentification de message (MAC) est ensuite calculé avec la fonction HMAC-SHA256 et la clé 2. Il couvre le nom de champ, l'IV de champ et le cryptogramme de champ. Enfin, l'ensemble de valeurs MAC de champ distinctes est lié, et leur MAC est calculé avec la fonction HMAC-SHA256 et la clé 3. Le MAC 256 bits est stocké avec les données chiffrées. Les 128 premiers bits de ce MAC servent d'identificateur d'enregistrement.

Cet enregistrement chiffré est ensuite stocké dans la base de données publique CloudKit sous l'identificateur d'enregistrement. Il n'est jamais muté, et chaque fois que l'utilisateur modifie son nom et sa photo, un nouvel enregistrement chiffré est généré. Lorsque l'utilisateur 1 choisit de partager son nom et sa photo avec l'utilisateur 2, il envoie la clé d'enregistrement avec l'identificateur d'enregistrement à l'intérieur de l'entité iMessage chiffrée.

Lorsque l'appareil de l'utilisateur 2 reçoit cette entité iMessage, il remarque qu'elle contient un identificateur d'enregistrement et une clé de surnom et de photo. L'appareil de l'utilisateur 2 accède ensuite à la base de données publique CloudKit pour récupérer le nom et la photo chiffrés sous l'identifiant d'enregistrement et l'envoie au moyen d'iMessage.

Une fois le message récupéré, l'appareil de l'utilisateur 2 déchiffre l'entité et vérifie la signature directement à l'aide de l'identificateur d'enregistrement. Si la signature passe la vérification, l'utilisateur 2 obtient le nom et la photo, et il peut choisir de l'ajouter à ses contacts ou de l'utiliser pour Messages.

Clavardage commercial sécurisé avec l’app Messages

Le clavardage commercial est un service de messagerie qui permet à l’utilisateur de communiquer avec une entreprise au moyen de l’app Messages. Avec le clavardage commercial, l’utilisateur contrôle toujours la conversation. Il peut aussi supprimer la conversation et bloquer l’entreprise pour l’empêcher de communiquer avec lui à l’avenir. À des fins de confidentialité, l’entreprise ne reçoit ni le numéro de téléphone de l’utilisateur, ni son adresse courriel, ni les informations de son compte iCloud. Un identifiant unique spécial appelé *identifiant opaque* est généré par l’IDS (Apple Identity Service, service d’identité d’Apple) et transmis à l’entreprise. L’identifiant opaque est unique à la relation entre l’identifiant Apple de l’utilisateur et l’identifiant de l’entreprise. Un utilisateur a un identifiant opaque différent pour chaque entreprise qu’il contacte par l’entremise du clavardage commercial. L’utilisateur a le choix de partager des informations personnelles qui permettent de l’identifier avec l’entreprise.

Le clavardage commercial est compatible avec les identifiants Apple gérés à partir d’Apple Business Manager et détermine s’ils sont activés pour iMessage et FaceTime dans Apple School Manager.

Les messages envoyés à l’entreprise sont chiffrés entre les appareils des utilisateurs et les serveurs de messagerie d’Apple, et utilisent la même sécurité et les mêmes serveurs de messagerie d’Apple que les iMessages. Les serveurs de messagerie d’Apple déchiffrent ces messages dans la mémoire vive et les transmettent à l’entreprise au moyen d’un lien chiffré qui utilise le protocole TLS 1.2. Les messages ne sont jamais stockés d’une façon non chiffrée lorsqu’ils transitent par le service de clavardage commercial d’Apple. Les réponses des entreprises sont également envoyées au moyen du protocole TLS 1.2 aux serveurs de messagerie d’Apple, où elles sont chiffrées au moyen des clés publiques uniques de chacun des appareils du destinataire.

Si les appareils de l’utilisateur sont en ligne, le message est distribué immédiatement et n’est pas mis en cache sur les serveurs de messagerie d’Apple. Si l’appareil de l’utilisateur n’est en ligne, le message chiffré est mis en cache pour une durée maximale de 30 jours pour permettre à l’utilisateur de le recevoir lorsque son appareil sera de nouveau en ligne. Dès que l’appareil est de nouveau en ligne, le message est distribué et supprimé du cache. Après 30 jours, le message non distribué qui a été mis en cache expire et est définitivement supprimé.

Le service de clavardage commercial ne stocke jamais les historiques de conversation.

Sécurité de FaceTime

FaceTime est le service d’appels audio et vidéo d’Apple. Comme iMessage, les appels FaceTime utilisent le service de notifications Push d’Apple (APN) pour établir une première connexion aux appareils enregistrés de l’utilisateur. Le contenu audiovisuel des appels FaceTime est protégé par un système de chiffrement de bout en bout, afin que personne d’autre que l’expéditeur et le destinataire ne puisse y accéder. Apple n’est pas en mesure de déchiffrer ces données.

La connexion FaceTime initiale se fait au moyen d'une infrastructure de serveurs Apple qui relaient les paquets de données entre les appareils enregistrés des utilisateurs. Des notifications APN et des messages STUN pour NAT servent à vérifier les certificats d'identité des appareils et un secret partagé est défini pour chaque session. Le secret partagé est utilisé pour dériver les clés de session des canaux multimédias diffusées à l'aide du protocole SRTP (Secure Real-time Transport Protocol). Les paquets SRTP sont chiffrés à l'aide de l'algorithme AES256 en mode compteur et de la fonction HMAC-SHA1. À la suite de la connexion initiale et de la configuration de sécurité, FaceTime utilise STUN et ICE (Interactive Connectivity Establishment) pour établir une connexion pair à pair entre les appareils, si possible.

FaceTime en groupe permet de passer des appels qui comptent jusqu'à 33 correspondants simultanément. Tout comme les appels FaceTime typiques en tête-à-tête, les appels en groupe sont chiffrés de bout en bout sur l'appareil de chaque correspondant. Bien que les appels FaceTime en groupe réutilisent la majorité de l'infrastructure et de la conception de FaceTime en tête-à-tête, ils reposent sur un nouveau mécanisme d'établissement de clés qui s'ajoute à l'authenticité fournie par le service d'identité d'Apple (IDS). Ce protocole est source de confidentialité persistante, c'est-à-dire que le détournement de l'appareil d'un utilisateur n'induit pas la divulgation du contenu des appels passés. Les clés de session sont enveloppées par l'algorithme AES-SIV et distribuées auprès des correspondants au moyen d'une construction ECIES avec des clés éphémères P-256 ECDH.

Lorsque de nouveaux numéros de téléphone ou de nouvelles adresses courriel sont ajoutés à un appel FaceTime en groupe en cours, les appareils actifs génèrent de nouvelles clés de support et ne partagent en aucun cas les clés utilisées précédemment avec les appareils récemment ajoutés.

App Localiser

Sécurité de Localiser

Aperçu

L'app Localiser combine Localiser mon iPhone et Localiser mes amis dans une seule et même app pour iOS, iPadOS et macOS. Elle peut aider les utilisateurs à retrouver un appareil, même s'il s'agit d'un Mac hors ligne. Un appareil en ligne peut simplement signaler sa position à l'utilisateur par iCloud. L'app Localiser fonctionne hors ligne en envoyant, à partir de l'appareil égaré, des signaux Bluetooth à faible portée qui sont détectables par les autres appareils Apple utilisés à proximité. Ces appareils à proximité relaient ensuite la position de l'appareil égaré à iCloud afin que l'utilisateur puisse le localiser dans l'app Localiser, tout en protégeant la confidentialité et la sécurité de tous les utilisateurs concernés. L'app Localiser fonctionne même avec un Mac hors ligne et en veille.

À l'aide de Bluetooth et des centaines de millions d'appareils iOS, iPadOS et macOS utilisés partout dans le monde, l'utilisateur peut retrouver un appareil même s'il ne peut pas se connecter à un réseau Wi-Fi ou cellulaire. N'importe quel appareil iOS, iPadOS ou macOS pour lequel la « recherche hors ligne » est activée dans les réglages de l'app Localiser peut servir d'appareil « chercheur ». Ainsi, l'appareil peut détecter la présence d'un appareil perdu hors ligne à l'aide du Bluetooth, puis utiliser sa connexion réseau pour signaler sa position approximative au propriétaire. Lorsque la recherche hors ligne est activée pour un appareil, cela signifie également qu'il peut être localisé par d'autres participants de la même façon. Cette interaction est entièrement chiffrée de bout en bout, anonyme et conçue pour économiser la batterie et les données. Ses répercussions sur l'autonomie de la batterie et l'utilisation du forfait de données cellulaires sont donc minimes et la confidentialité de l'utilisateur est protégée.

Remarque : L'app Localiser pourrait ne pas être offerte dans certains pays ou certaines régions.

Chiffrement de bout en bout

L'app Localiser repose sur la cryptographie à clé publique avancée. Lorsque la recherche hors ligne est activée dans les réglages de l'app Localiser, une paire de clés de chiffrement privée EC (courbes elliptiques) P-224 est générée directement sur l'appareil. Elle est notée {d,P}, où *d* est la clé privée et *P*, la clé publique. De plus, un SK_0 secret de 256 bits et un compteur $_i$ sont réglés à zéro. Cette paire de clés privée et le secret ne sont jamais transmis à Apple et sont uniquement synchronisés entre les autres appareils de l'utilisateur d'une manière chiffrée de bout en bout à l'aide du trousseau iCloud. Le secret et le compteur sont utilisés pour dériver la clé symétrique SK_i courante selon la construction récursive suivante : $SK_i = KDF(SK_{i-1}, \text{“update”})$.

Basés sur la clé SK_i, deux grands entiers u_i et v_i sont calculés par la formule $(u_i,v_i) = KDF(SK_i, \text{“diversify”})$. Tant la clé privée P-224 (*d*) que la clé publique correspondante (*P*) sont ensuite dérivées au moyen d'une relation affine qui implique le calcul d'une paire de clés éphémères à partir des deux nombres entiers : la clé privée dérivée est d_i, où $d_i = u_i * d + v_i$ (modulo le degré de la courbe P-224). La partie publique correspondante est P_i et vérifie que $P_i = u_i * P + v_i * G$.

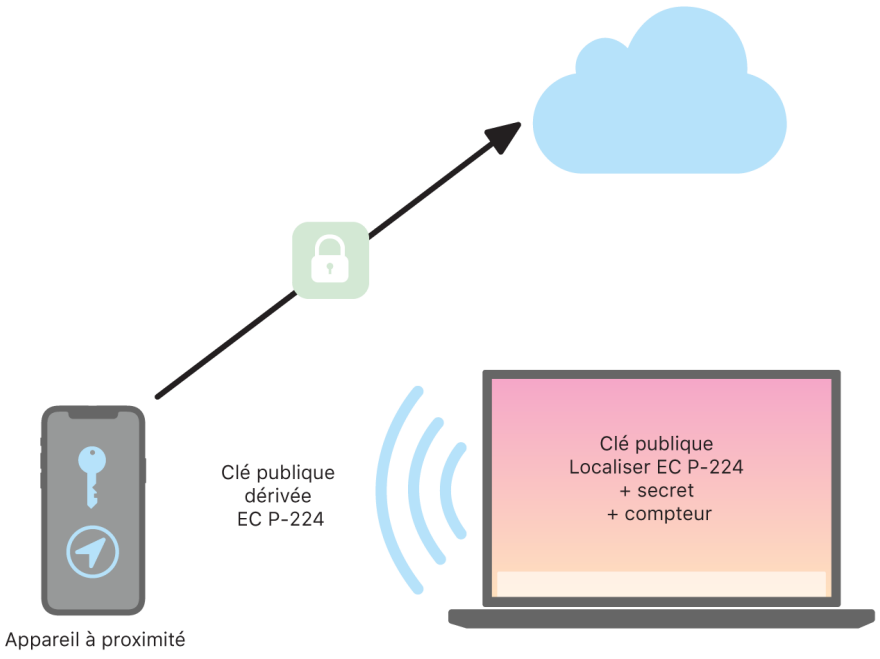
Lorsqu'un appareil est égaré et qu'il ne peut pas se connecter à un réseau Wi-Fi ou cellulaire (par exemple un MacBook Pro laissé sur un banc de parc), il commence à diffuser périodiquement la clé publique dérivée P_i pour une période limitée dans une entité Bluetooth. P-224 fait en sorte qu'une seule entité Bluetooth suffise pour contenir la représentation de la clé publique. Les appareils à proximité peuvent ensuite participer à la localisation de l'appareil hors ligne en chiffrant sa position dans la clé publique. Environ toutes les 15 minutes, la clé publique est remplacée à l'aide d'une valeur incrémentée du compteur et du processus expliqué ci-dessus afin que l'utilisateur ne puisse pas être suivi par un identifiant pérenne. Le mécanisme de dérivation est conçu pour empêcher les différentes clés publiques P_i d'être liées au même appareil.

Protection de l’anonymat des utilisateurs et des appareils

Outre le chiffrement des données de localisation et d’autres données, d’autres mesures assurent la protection de l’anonymat des utilisateurs et des appareils. Tout d’abord, l’identité des participants n’est divulguée à personne, pas même à Apple. Le contenu et les en-têtes des données transmises à Apple par les appareils chercheurs ne contiennent aucune information d’authentification. Par conséquent, Apple ne connaît pas l’identité du propriétaire de l’appareil chercheur ni de celui de l’appareil trouvé. De plus, Apple ne consigne aucun renseignement qui pourrait révéler l’identité du propriétaire de l’appareil chercheur et ne conserve aucune information qui pourrait permettre à quelqu’un d’établir une corrélation entre ce dernier et le propriétaire de l’appareil trouvé. Le propriétaire de l’appareil trouvé reçoit uniquement les données de localisation chiffrées qui sont déchiffrées et affichées dans l’app Localiser, sans renseignement sur la personne ayant trouvé l’appareil.

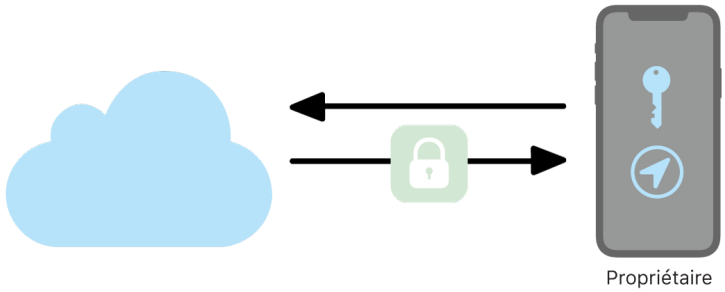
Utilisation de Localiser pour chercher les appareils Apple égarés

Tout appareil Apple à portée Bluetooth pour lequel la recherche hors ligne est activée peut détecter un signal provenant d’un autre appareil Apple configuré pour autoriser Localiser et lire la clé P_i diffusée. À l’aide d’une construction ECIES et de la clé publique P_i diffusée, les appareils chercheurs chiffrent leurs données de localisation actuelles et les relaient à Apple. La position chiffrée est associée à un index de serveur qui est calculé alors que l’entité Bluetooth fournit le hachage SHA256 de la clé publique P-224 P_i. Apple ne détient jamais la clé de déchiffrement, donc elle ne peut pas lire la position chiffrée par l’appareil chercheur. Le propriétaire de l’appareil égaré peut reconstruire l’index et déchiffrer la position.



Localisation des appareils par l’app Localiser.

Pendant la tentative de localisation de l'appareil égaré, une plage de valeurs de compteur est estimée pour la période de recherche. Une fois qu'il connaît la clé privée P-224 *d* d'origine et les valeurs secrètes SK_i sur la plage de valeurs de compteur de la période de recherche, le propriétaire peut reconstruire l'ensemble de valeurs $\{d_i, SHA256(P_i)\}$ pour la totalité de la période de recherche. L'appareil du propriétaire utilisé pour localiser l'appareil égaré peut ensuite effectuer des requêtes auprès du serveur à l'aide de l'ensemble de valeurs indices $SHA256(P_i)$ et télécharger les positions chiffrées. Ensuite, l'app Localiser déchiffre localement les positions avec les clés privées d_i correspondantes et indique la position approximative de l'appareil égaré. Les rapports de localisation de plusieurs appareils chercheurs sont combinés par l'app du propriétaire pour augmenter la précision de la position.



Obtention de la position de l'appareil par le propriétaire dans l'app Localiser

Localisation d'appareils hors ligne

Lorsque la fonctionnalité Localiser mon iPhone est activée sur un appareil, la recherche hors ligne est activée par défaut au moment où l'utilisateur effectue une mise à niveau vers iOS 13, iPadOS 13.1, macOS 10.15 ou une version ultérieure de ces systèmes d'exploitation. Cela vise à donner à tous les utilisateurs les meilleures chances de retrouver un appareil égaré. Cependant, l'utilisateur peut en tout temps désactiver la recherche hors ligne dans les réglages de l'app Localiser sur son appareil s'il préfère ne pas participer. Lorsque la recherche hors ligne est désactivée, l'appareil ne sert plus de chercheur et n'est plus détectable par d'autres appareils chercheurs. Toutefois, l'utilisateur peut quand même localiser l'appareil s'il est connecté à un réseau Wi-Fi ou cellulaire.

Lorsqu'un appareil hors ligne égaré est localisé, l'utilisateur reçoit une notification et un courriel qui l'avisent que son appareil a été trouvé. Pour afficher la position de l'appareil égaré, l'utilisateur ouvre l'app Localiser et sélectionne l'onglet Appareils. Plutôt que d'afficher l'appareil sur un plan vierge, comme cela aurait été le cas avant qu'il soit retrouvé, l'app Localiser affiche une position sur le plan avec une adresse approximative et des informations sur le temps écoulé depuis la détection de l'appareil. Si d'autres rapports de localisation s'ajoutent à ceux reçus, la position actuelle, la date et l'heure sont automatiquement mises à jour. Bien que les utilisateurs ne puissent pas faire sonner un appareil hors ligne ni l'effacer à distance, ils peuvent utiliser les données de localisation pour revenir sur leurs pas ou prendre d'autres mesures pour le récupérer.

Continuité

Aperçu de la sécurité de Continuité

Les fonctionnalités de continuité reposent sur des technologies comme iCloud, Bluetooth et Wi-Fi pour permettre aux utilisateurs de poursuivre sur un deuxième appareil une activité entamée sur un premier, de passer et de recevoir des appels téléphoniques, d'échanger des messages texte et de partager une connexion Internet par réseau cellulaire.

Sécurité de Handoff

Aperçu

Avec la fonctionnalité Handoff, lorsque les appareils iOS, iPadOS et macOS d'un utilisateur sont à proximité les uns des autres, l'utilisateur peut transférer son activité d'un appareil à l'autre instantanément.

Lorsqu'un utilisateur se connecte à iCloud sur un deuxième appareil prenant en charge Handoff, les deux appareils établissent un jumelage hors bande Bluetooth faible énergie (BLE) 4.2 au moyen du service de notifications Push d'Apple (APN). Les messages sont chiffrés comme ceux d'iMessage. Une fois les appareils jumelés, chacun génère une clé symétrique AES 256 bits qui est ensuite stockée dans son trousseau. Cette clé peut chiffrer et authentifier les notifications BLE qui communiquent l'activité actuelle de l'appareil aux autres appareils jumelés via iCloud à l'aide d'un algorithme AES256 en mode GCM, avec des mesures de protection antirejeu.

La première fois qu'un appareil reçoit une notification provenant d'une nouvelle clé, il établit une connexion BLE à l'appareil émetteur et exécute un échange de clés de chiffrement de notification. Cette connexion est sécurisée par chiffrement BLE 4.2 standard ainsi que par un chiffrement des messages distincts (comme dans iMessage). Dans certaines situations, ces messages sont envoyés par le service APN plutôt que BLE. Les données utiles de l'activité sont protégées et transférées de la même manière qu'un message iMessage.

Handoff entre sites Web et apps natives

La fonctionnalité Handoff permet à une app iOS, iPadOS ou macOS native de reprendre l'activité de l'utilisateur sur une page Web appartenant à des domaines contrôlés de manière légitime par le développeur de l'app. Elle permet également la reprise dans un navigateur Web de l'activité d'un utilisateur dans l'app native.

Pour aider à éviter que des apps natives ne reprennent des sites Web non contrôlés par le développeur, l'app concernée doit prouver qu'elle contrôle légitimement les domaines qu'elle souhaite reprendre. Le contrôle d'un domaine de site Web est établi par le même mécanisme utilisé pour les accréditations Web partagées. Pour en savoir plus, consultez la section Accès des apps aux mots de passe enregistrés. Le système doit valider le contrôle de l'app sur le nom de domaine avant que l'app ne soit autorisée à accepter la transmission de l'activité de l'utilisateur.

N'importe quel navigateur ayant adopté les API Handoff peut servir de source de transmission de page Web. Lorsque l'utilisateur consulte une page Web, le système diffuse le nom de domaine de cette page dans les octets de notification Handoff chiffrés. Seuls les autres appareils de l'utilisateur sont capables de déchiffrer les octets de notification.

Sur l'appareil récepteur, le système détecte qu'une app native installée accepte la transmission du nom de domaine annoncé et affiche l'icône de cette app native comme option de transmission Handoff. Une fois ouverte, l'app native reçoit l'URL complète et le titre de la page Web. Aucune autre information n'est transmise du navigateur à l'app native.

En sens inverse, une app native peut spécifier une URL de reprise lorsqu'un appareil récepteur Handoff ne possède pas la même app native installée. Dans ce cas, le système affiche le navigateur par défaut de l'utilisateur en tant que possibilité d'app Handoff (si le navigateur a adopté les API Handoff). Lorsque la transmission est demandée, le navigateur s'ouvre et reçoit l'URL de reprise fournie par l'app source. L'URL de reprise ne doit pas nécessairement être limitée aux noms de domaine contrôlés par le développeur de l'app native.

Transmission de volumes de données plus importants

Outre les fonctionnalités de base de Handoff, certaines apps peuvent choisir d'utiliser des API prenant en charge l'envoi de volumes de données plus importants par l'intermédiaire d'une technologie Wi-Fi pair-à-pair créée par Apple (comme avec AirDrop). L'app Mail, par exemple, utilise ces API pour prendre en charge la transmission par Handoff de brouillons de message susceptibles d'inclure des pièces jointes volumineuses.

Lorsqu'une app exploite cette possibilité, l'échange entre les deux appareils démarre comme une transmission Handoff normale. Toutefois, après la réception du contenu initial par BLE, l'appareil récepteur ouvre une nouvelle connexion via Wi-Fi. Cette connexion est chiffrée (par TLS), ce qui implique l'échange des certificats d'identité iCloud des appareils. L'identité des certificats est comparée à l'identité de l'utilisateur. Le reste des données utiles est envoyé à travers cette connexion chiffrée jusqu'à ce que le transfert soit terminé.

Presse-papiers universel

Le presse-papiers utilise Handoff pour transférer de façon sécurisée le contenu du presse-papiers de l'utilisateur sur tous ses appareils, ce qui permet de copier le contenu d'un appareil et de le coller sur un autre. Le contenu est protégé comme le sont les autres données Handoff et partagé par défaut par le presse-papiers universel, à moins que le développeur de l'app ne choisisse de désactiver le partage.

Les apps ont accès aux données du presse-papiers, que l'utilisateur ait collé le presse-papiers dans l'app ou non. Avec le presse-papiers universel, cet accès aux données s'étend aux apps exécutées sur les autres appareils de l'utilisateur (connectés à iCloud).

Sécurité du relais des appels cellulaires de l'iPhone

Si le Mac, l'iPad, l'iPod touch ou le HomePod d'un utilisateur est connecté au même réseau Wi-Fi que son iPhone, l'utilisateur peut passer et recevoir des appels téléphoniques via la connexion cellulaire de l'iPhone. Les appareils doivent être connectés à la fois à iCloud et à FaceTime avec le même identifiant Apple.

À la réception d'un appel, tous les appareils configurés sont notifiés par l'intermédiaire du service de notifications Push d'Apple (APN), chaque notification utilisant le même chiffrement de bout en bout qu'iMessage. Les appareils qui sont connectés au même réseau affichent alors l'interface utilisateur de notification d'appel entrant. Lorsque l'utilisateur répond à l'appel, le son est transmis en toute fluidité à partir de l'iPhone de l'utilisateur au moyen d'une connexion pair-à-pair sécurisée entre les deux appareils.

Si un appel est pris sur un appareil, la sonnerie est coupée sur les appareils à proximité et jumelés via iCloud par une brève notification Bluetooth faible énergie (BLE) 4.0. Les octets de cette notification sont chiffrés par la même méthode que les notifications de type Handoff.

Les appels sortants sont également relayés vers l'iPhone par le service APN, et le son est diffusé de la même façon par la liaison pair à pair sécurisée entre les appareils. Il est possible de désactiver le relais d'appels téléphoniques sur un appareil en désactivant l'option « Appels cellulaires iPhone » dans les réglages FaceTime.

Sécurité du transfert de SMS de l'iPhone

Le transfert de SMS envoie automatiquement les messages texte reçus sur iPhone à l'iPad, à l'iPod touch ou au Mac inscrit d'un utilisateur. Chaque appareil doit être connecté au service iMessage avec le même identifiant Apple. Lorsque le transfert de SMS est activé, l'inscription au service est automatique sur les appareils qui appartiennent au cercle de confiance de l'utilisateur si l'authentification à deux facteurs est activée. Autrement, l'inscription est validée sur chaque appareil par la saisie d'un code numérique aléatoire à six chiffres généré par l'iPhone.

Une fois que les appareils sont liés, l'iPhone chiffre les SMS entrants et les transfère à chaque appareil en faisant appel aux méthodes décrites dans la section Aperçu de la sécurité d'iMessage. Les réponses sont renvoyées à l'iPhone selon les mêmes méthodes, puis l'iPhone envoie la réponse sous forme de message texte en utilisant le mécanisme de transmission de SMS de l'opérateur. Le transfert de SMS peut être activé ou désactivé dans les réglages de Messages.

Sécurité d'Instant Hotspot

Instant Hotspot connecte d'autres appareils Apple au partage de connexion iOS ou iPadOS. Les appareils iOS et iPadOS prenant en charge Instant Hotspot utilisent Bluetooth faible énergie (BLE) pour détecter les appareils connectés au même compte iCloud ou aux comptes utilisés avec le partage familial (sous iOS 13 et iPadOS) et communiquer avec eux. Les Mac compatibles, sous OS X 10.10 et les versions ultérieures, utilisent la même technologie pour détecter, et communiquer avec, les appareils iOS et iPadOS prenant en charge Instant Hotspot.

Lorsqu'un utilisateur accède aux réglages Wi-Fi d'un appareil, ce dernier émet une notification BLE contenant un identifiant reconnu par tous les autres appareils connectés au même compte iCloud. L'identifiant est généré à partir d'un identifiant Destination Signaling Identifier (DSID) lié au compte iCloud et remplacé périodiquement. Lorsque d'autres appareils connectés au même compte iCloud et prenant en charge le partage de connexion se trouvent à proximité, ils détectent le signal et y répondent en indiquant leur disponibilité à utiliser Instant Hotspot.

Lorsqu'un utilisateur qui ne participe pas au partage familial choisit un iPhone ou un iPad pour le partage de connexion, une requête d'activation du partage de connexion est envoyée à cet appareil. La requête, chiffrée à l'aide d'une méthode de chiffrement similaire à celle d'iMessage, est envoyée via une liaison chiffrée par BLE. L'appareil répond ensuite via la même liaison BLE, en utilisant la même méthode de chiffrement par message avec les informations du partage de connexion.

Pour les utilisateurs qui font partie du partage familial, les informations du partage de connexion sont partagées de façon sécurisée au moyen d'un mécanisme semblable à celui utilisé par les appareils HomeKit pour la synchronisation des informations. Plus particulièrement, la connexion qui transmet les informations du partage de connexion entre les utilisateurs est sécurisées à l'aide d'une clé éphémère ECDH (Curve25519) authentifiée avec les clés publiques Ed25519 propres aux appareils des utilisateurs. Les clés publiques utilisées sont celles qui ont été synchronisées auparavant entre les membres du partage familial à l'aide de l'IDS lors de l'établissement du partage familial.

Sécurité des clés de véhicule sous iOS

Aperçu

Les clés de véhicule sont prises en charge nativement par les appareils iPhone compatibles et les appareils Apple Watch jumelés. Elles se présentent sous forme de cartes (créées par Apple pour le compte du constructeur automobile) dans l'app Wallet et prennent en charge le cycle de vie complet des cartes Apple Pay (mode Perdu iCloud, effacement à distance, suppression locale de la carte et option « Effacer contenu et réglages »). En plus de la gestion standard des cartes Apple Pay, les cartes de véhicule partagées peuvent être supprimées de l'iPhone ou de l'Apple Watch du propriétaire, et de l'interface humain-machine du véhicule.

Les clés de véhicule peuvent être utilisées pour déverrouiller, verrouiller ou démarrer un véhicule et régler son mode de conduite. La « transaction standard » donne lieu à une authentification mutuelle et est obligatoire pour que le moteur démarre. Les transactions de déverrouillage et de verrouillage peuvent utiliser la « transaction rapide » lorsque des raisons de performance le requièrent.

Les clés sont créées en jumelant un iPhone avec un véhicule compatible qui appartient à l'utilisateur. Toutes les clés sont créées sur le Secure Element intégré sur la base d'une génération ECC-OBKG (Elliptic Curve Cryptography On-board Key Generation, génération de clés embarquée par cryptographie sur les courbes elliptiques [NIST P-256]), et les clés privées ne quittent jamais le Secure Element. Les appareils et le véhicule utilisent la communication en champ proche (CCP), et la gestion de la clé utilise une API de serveur Apple-constructeur automobile au moyen d'un protocole TLS mutuellement authentifié. Une fois qu'une clé est jumelée à un iPhone, toute Apple Watch jumelée à cet iPhone peut aussi recevoir la clé. Lorsqu'une clé est supprimée soit sur le véhicule soit sur l'appareil, elle ne peut pas être restaurée. Les clés qui se trouvent sur des appareils égarés ou volés peuvent être suspendues et réactivées, mais leur transfert sur un nouvel appareil requiert un nouveau jumelage ou un nouveau partage.

Jumelage par le propriétaire

Le propriétaire doit prouver qu'il possède le véhicule (le processus varie selon le constructeur automobile) et peut commencer le processus de jumelage dans l'app du constructeur automobile, à partir d'un lien envoyé dans un courriel par le constructeur automobile, ou à partir du menu du véhicule. Dans tous les cas, le propriétaire doit présenter à l'iPhone un mot de passe de jumelage à usage unique confidentiel qui sert à générer un canal de jumelage sécurisé au moyen du protocole SPAKE2+ avec courbe NIST P-256. Lors de l'utilisation de l'app ou du lien reçu par courriel, le mot de passe est automatiquement transféré à l'iPhone, tandis qu'il doit être entré manuellement lorsque le jumelage est amorcé à partir du véhicule.

Partage de clés

L'iPhone jumelé du propriétaire de véhicule peut partager des clés avec les iPhone admissibles de ses proches ou amis (et avec les Apple Watch jumelées) en envoyant une invitation spécifique à l'appareil au moyen d'iMessage et du service d'identité d'Apple (IDS). Toutes les commandes de partage sont échangées au moyen de la fonction IDS chiffrée de bout en bout. L'iPhone jumelé du propriétaire empêche le canal IDS de changer pendant le processus de partage.

Sur acceptation de l'invitation, l'iPhone du proche ou de l'ami du propriétaire crée une clé numérique et renvoie la chaîne du certificat de création de la clé à l'iPhone jumelé du propriétaire pour vérifier que la clé a été créée sur un appareil Apple authentique. L'iPhone jumelé du propriétaire signe la clé publique ECC de l'iPhone du proche ou de l'ami et renvoie la signature à l'iPhone en question. L'opération de signature dans l'appareil du propriétaire requiert l'authentification de l'utilisateur (au moyen de Touch ID, de Face ID ou de la saisie du code) et l'intention sécurisée de l'utilisateur, comme décrite dans la section Utilisations de Touch ID et de Face ID. L'autorisation est requise lors de l'envoi de l'invitation, puis est stockée dans le Secure Element pour être utilisée lorsque l'appareil de l'ami renvoie la demande de signature.

Suppression de clés

Les clés peuvent être supprimées de l'appareil de leur détenteur à partir du véhicule ou de l'appareil de son propriétaire. L'effet de toute suppression effectuée sur l'iPhone du détenteur de la clé est immédiat, même si ce dernier est en train d'utiliser la clé. Par conséquent, une mise en garde sérieuse s'affiche avant que vous ne puissiez procéder à la suppression.

Pour les suppressions de clés effectuées à partir du véhicule, le constructeur automobile peut exiger que le véhicule soit en ligne pour procéder.

Dans les deux cas, la suppression effectuée sur l'appareil du détenteur de la clé ou sur le véhicule est communiquée à un serveur d'inventaire de clés (KIS) du constructeur automobile. Ce serveur enregistre les clés émises pour un véhicule donné à des fins d'assurance.

Le propriétaire peut demander une suppression à partir du verso de sa carte. La demande est d'abord envoyée au constructeur automobile pour procéder à la suppression de la clé dans le véhicule. Les conditions de suppression de la clé du véhicule sont établies par le constructeur automobile. Ce n'est qu'une fois la clé supprimée du véhicule que le serveur du constructeur automobile envoie une demande de suppression à l'appareil du détenteur de la clé.

Lorsqu'une clé est supprimée d'un appareil, l'applet qui gère les clés de véhicule numériques émet une attestation de suppression signée de façon cryptographique, qui sert de preuve de suppression par le constructeur automobile et qui est utilisée pour supprimer la clé du KIS.

Transactions standard

Un canal sécurisé entre le lecteur et un iPhone est initialisé en générant des paires de clés éphémères sur le lecteur et sur l'iPhone. Au moyen d'une méthode d'échange de clés, un secret partagé peut être dérivé de part et d'autre et utilisé pour générer une clé symétrique partagée au moyen d'un protocole d'échange de clés Diffie-Hellman, une fonction de dérivation de clés et des signatures provenant de la clé longue durée établie lors du jumelage.

La clé publique éphémère générée par le véhicule est signée par la clé longue durée privée du lecteur. Cela permet à l'iPhone d'authentifier le lecteur. Du point de vue de l'iPhone, ce protocole est conçu pour empêcher la divulgation de données sensibles et confidentielles à tout adversaire qui intercepterait la communication.

Enfin, l'iPhone utilise le canal sécurisé établi pour chiffrer l'identifiant de sa clé publique ainsi que la signature calculée à partir d'un défi dérivé des données du lecteur et de certaines données précises qui se rapportent à l'app. Cette vérification de la signature de l'iPhone par le lecteur permet à ce dernier d'authentifier l'appareil.

Transactions rapides

L'iPhone génère un cryptogramme basé sur un secret précédemment partagé au cours d'une transaction standard. Ce cryptogramme permet au véhicule d'authentifier rapidement l'appareil dans les cas où les performances sont essentielles. Facultativement, un canal sécurisé est établi entre le véhicule et l'appareil en dérivant les clés de session à partir d'un secret précédemment partagé au cours d'une transaction standard et d'une paire de clés éphémères. C'est la capacité du véhicule à établir un canal sécurisé qui l'authentifie auprès de l'iPhone.

Confidentialité

Le KIS du constructeur automobile ne stocke aucune des données suivantes : identifiant de l'appareil, SEID ou identifiant Apple. Il stocke uniquement un identifiant mutable, l'identifiant de l'autorité de certification de l'instance. Cet identifiant n'est lié à aucune donnée privée dans l'appareil ou par le serveur, et il est supprimé lorsque l'utilisateur efface complètement son appareil (au moyen de l'option « Effacer contenu et réglages »).

Sécurité des réseaux

Aperçu de la sécurité des réseaux

En plus des dispositifs qu'Apple intègre à ses appareils pour protéger les données qui y sont stockées, les entreprises disposent de nombreuses mesures pour assurer la sûreté des données qu'un appareil reçoit et envoie. Toutes ces protections et mesures appartiennent à la sécurité des réseaux.

Comme les utilisateurs doivent pouvoir accéder aux réseaux d'entreprise où qu'ils soient dans le monde, il est important de veiller à ce qu'ils soient bel et bien autorisés, et à ce que les données soient protégées durant leur transmission. Pour atteindre ces objectifs en matière de sécurité, iOS, iPadOS et macOS sont dotés de technologies éprouvées et souscrivent aux plus récentes normes relatives à la connexion aux réseaux Wi-Fi et cellulaires. C'est pourquoi nos systèmes d'exploitation font appel à des protocoles réseau standards – et les mettent à la disposition des développeurs – pour l'authentification, l'autorisation et le chiffrement des communications.

Sécurité TLS

iOS, iPadOS et macOS prennent en charge les protocoles Transport Layer Security (TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3) et Datagram Transport Layer Security (DTLS). Le protocole TLS prend en charge les algorithmes AES128 et AES256, et préfère les suites de chiffrement avec confidentialité persistante. Les apps qui se connectent à Internet, comme Safari, Calendrier et Mail, utilisent automatiquement ce protocole pour établir un canal de communication chiffré entre l'appareil et les services du réseau. Les API de haut niveau (comme CFNetwork) permettent aux développeurs d'intégrer facilement le protocole TLS à leurs apps, tandis que les API de bas niveau (comme Network.framework) leur offrent un contrôle plus fin. L'API CFNetwork rejette le protocole SSL 3; les apps qui utilisent WebKit, comme Safari, sont donc incapables d'établir une connexion SSL 3.

Sous iOS 11 et macOS 10.13 et les versions ultérieures, les certificats SHA-1 ne sont plus pris en charge pour les connexions TLS, à moins qu'ils ne soient autorisés par l'utilisateur. Les certificats dotés de clés RSA de moins de 2 048 bits sont aussi rejetés. La méthode de chiffrement symétrique RC4 n'est plus prise en charge sous iOS 10 et macOS 10.12. Par défaut, les clients TLS ou les serveurs utilisant les API SecureTransport ne sont pas compatibles avec la méthode de chiffrement RC4 et sont incapables de se connecter si RC4 est la seule méthode de chiffrement disponible. Les services ou les apps qui nécessitent RC4 devraient être mis à niveau et utiliser des méthodes de chiffrement sécurisées. Sous iOS 12.1, seuls les certificats délivrés après le 15 octobre 2018 à partir d'un certificat racine de confiance et inscrits sur une liste approuvée de transparence des certificats sont pris en charge pour les connexions TLS. Sous iOS 12.2, TLS 1.3 est activé par défaut pour les API Network.framework et NSURLSession. Les clients TLS qui utilisent les API SecureTransport ne peuvent pas utiliser TLS 1.3.

Fonctionnalité App Transport Security

La fonctionnalité App Transport Security établit des exigences de connexion par défaut afin que les apps se comportent conformément aux bonnes pratiques en matière de connexions sécurisées lorsqu'elles utilisent les API NSURLConnection, CFURL ou NSURLSession. Par défaut, App Transport Security restreint le choix des méthodes de chiffrement à celles qui offrent la confidentialité persistante, en particulier :

- ECDHE_ECDSA_AES et ECDHE_RSA_AES en mode GCM (Galois/Counter Mode)
- Mode CBC (Cipher Block Chaining, enchaînement des blocs)

Les apps peuvent désactiver l'exigence de confidentialité persistante par domaine, auquel cas le chiffrement RSA_AES est ajouté aux méthodes disponibles.

Les serveurs doivent prendre en charge TLS 1.2 et la confidentialité persistante, et les certificats doivent être valides et signés à l'aide de SHA256 ou mieux, avec une clé RSA de 2 048 bits ou une clé ECC de 256 bits minimum.

Les connexions réseau qui ne satisfont pas à ces exigences échouent, à moins que l'app annule App Transport Security. Les certificats non valides entraînent toujours une erreur permanente ou une absence de connexion. La fonctionnalité App Transport Security s'applique automatiquement aux apps compilées pour iOS 9 et macOS 10.11 et les versions ultérieures.

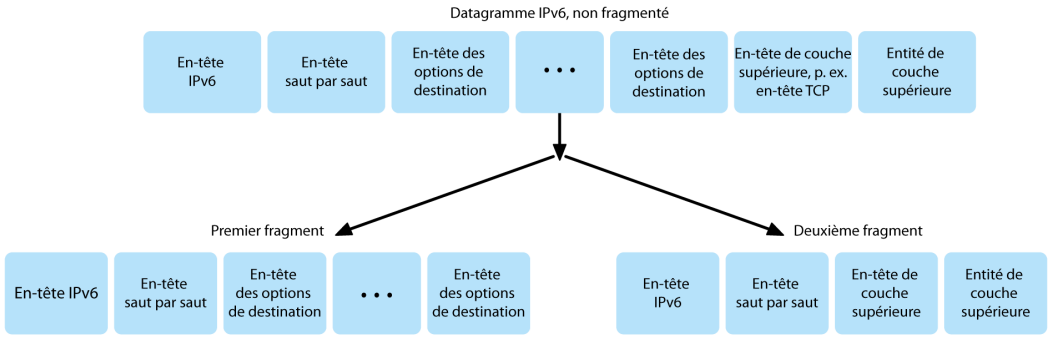
Vérification de la validité des certificats

L'évaluation de la fiabilité d'un certificat TLS est effectuée conformément aux normes établies par l'industrie, décrites dans le document RFC 5280, et comprend des normes émergentes comme RFC 6962 (sur la transparence des certificats). Sous iOS 11 et macOS 10.13 et les versions ultérieures, les appareils Apple sont mis à jour régulièrement avec la liste à jour des certificats révoqués ou restreints. Celle-ci est tirée des listes de révocation de certificats (CRL) publiées par chacune des autorités de certification racine intégrée autorisées par Apple et leurs émetteurs subordonnés. Apple peut, à sa discrétion, ajouter d'autres contraintes. Ces informations sont consultées dès qu'une fonction d'une API réseau est utilisée pour établir une connexion sécurisée. Si le nombre de certificats révoqués d'une autorité de certification est trop élevé pour les énumérer un par un, une évaluation de fiabilité pourrait plutôt nécessiter une réponse du protocole de vérification de certificats en ligne (OCSP), sans quoi elle échouerait.

Sécurité IPv6

Tous les systèmes d'exploitation Apple prennent en charge IPv6 et comptent sur plusieurs mécanismes pour protéger les renseignements personnels des utilisateurs et la stabilité de la pile réseau. Lorsque la SLAAC (Stateless Address Autoconfiguration, configuration automatique d'adresse sans état) est utilisée, les adresses IPv6 de toutes les interfaces sont générées d'une façon qui contribue à empêcher le pistage des appareils d'un réseau à l'autre et qui permet en même temps d'assurer une expérience d'utilisation de qualité en garantissant la stabilité de l'adresse lorsqu'aucun changement de réseau ne survient. L'algorithme de génération d'adresse repose sur des adresses générées de façon cryptographique conformément au document RFC 3972, amélioré par un modificateur propre à l'interface qui garantit que des interfaces différentes sur un même réseau finissent par avoir des adresses différentes. De plus, les adresses temporaires sont créées en privilégiant une durée de vie de 24 heures et sont utilisées par défaut pour toute nouvelle connexion. En harmonie avec la fonctionnalité Adresse Wi-Fi privée introduite dans iOS 14, iPadOS 14 et watchOS 7, une adresse lien-local unique est générée pour chaque réseau Wi-Fi auquel l'appareil se joint. Le SSID du réseau est incorporé comme un élément supplémentaire pour générer l'adresse, d'une façon semblable au paramètre Network_ID, conformément au document RFC 7217. Cette approche est utilisée dans iOS 14, iPadOS 14 et watchOS 7.

Pour prévenir les attaques qui reposent sur des en-têtes d'extension IPv6 et leur fragmentation, les appareils Apple implémentent les mesures de protection décrites dans les documents RFC 6980, RFC 7112 et RFC 8021. Ces mesures permettent entre autres de freiner les attaques au cours desquelles l'en-tête de la couche supérieure est trouvable uniquement dans le deuxième fragment (comme indiqué ci-dessous) et qui pourraient ensuite être une source d'ambiguïté pour les contrôles de sécurité, comme les filtres de paquets sans état.



Datagramme IPv6

De plus, pour contribuer à garantir la fiabilité de la pile IPv6 des systèmes d'exploitation Apple, les appareils Apple appliquent plusieurs limites aux structures de données liées à IPv6, telles que le nombre de préfixes par interface.

Sécurité des réseaux privés virtuels (VPN)

Les services réseau sécurisés comme les réseaux privés virtuels (VPN, Virtual Private Networks) exigent généralement une configuration minimale pour fonctionner sur les appareils iOS, iPadOS et macOS.

Protocoles pris en charge

Les appareils Apple sont compatibles avec les serveurs VPN prenant en charge les protocoles et méthodes d'authentification suivantes :

- IKEv2/IPsec avec authentification par secret partagé, certificats RSA ou ECDSA (Elliptic Curve Digital Signature Algorithm, algorithme de signature numérique basé sur les courbes elliptiques), EAP-MSCHAPv2 ou EAP-TLS;
- VPN-SSL avec l'app client adéquate provenant de l'App Store;
- L2TP/IPsec avec authentification par mot de passe MS-CHAPV2 et authentification machine par secret partagé (iOS, iPadOS et macOS) et RSA SecurID ou CRYPTOCard (macOS uniquement);
- Cisco IPsec avec authentification par mot de passe, RSA SecurID ou CRYPTOCard, et authentification machine par secret partagé et certificats (macOS uniquement).

Déploiements de VPN pris en charge

iOS, iPadOS et macOS prennent en charge les fonctions ci-dessous :

- *VPN sur demande :* pour les réseaux qui utilisent une authentification par certificat. Les politiques des TI précisent alors les domaines exigeant une connexion de ce type via un profil de configuration VPN.
- *VPN par app :* pour permettre une gestion beaucoup plus détaillée des connexions VPN. Les solutions de gestion des appareils mobiles (GAM) peuvent attribuer une connexion VPN à chaque app gérée ou à des domaines précis dans Safari. Cette mesure permet de veiller à ce que les données sécurisées transitent toujours sur le réseau de l'entreprise, et à ce que les données personnelles des utilisateurs en soient exclues.

iOS et iPadOS prennent en charge les fonctions ci-dessous :

- *VPN permanent :* peut être configuré sur les appareils gérés par une solution de GAM et supervisés à l'aide d'Apple Configurator 2, d'Apple School Manager ou Apple Business Manager. Les utilisateurs n'ont alors plus besoin d'activer le VPN pour protéger l'appareil lorsqu'ils se connectent à des réseaux cellulaires et à des réseaux Wi-Fi. Le VPN permanent donne à une entreprise le plein contrôle sur le trafic des appareils en dirigeant tout le trafic IP jusqu'à elle. Avec l'échange par défaut de paramètres et de clés pour le chiffrement suivant, le protocole IKEv2 sécurise la transmission du trafic en chiffrant les données. L'entreprise peut surveiller et filtrer le trafic entrant et sortant de ses appareils, sécuriser les données au sein de son réseau et limiter l'accès des appareils à Internet.

Sécurité Wi-Fi

Sécurité des protocoles

Accès sécurisé aux réseaux sans fil

Toutes les plateformes Apple prennent en charge les protocoles standards d'authentification Wi-Fi et de chiffrement pour fournir un accès authentifié et confidentiel lors de la connexion aux réseaux sans fil sécurisés suivants :

- Protocole WPA2 Personal
- Protocole WPA2 Enterprise
- Protocole WPA2/WPA3 Transitional
- Protocole WPA3 Personal
- Protocole WPA3 Enterprise
- Protocole WPA3 Enterprise avec chiffrement 192 bits

Les protocoles WPA2 et WPA3 authentifient chaque connexion et utilisent un chiffrement AES 128 bits pour veiller à la confidentialité des données transmises sans fil. Cela garantit aux utilisateurs une protection maximale des données lorsqu'ils envoient ou reçoivent sur un réseau Wi-Fi.

Prise en charge du protocole WPA3

Le protocole WPA3 est pris en charge par les appareils Apple suivants :

- iPhone 7 et modèles plus récents;
- iPad 5e génération et modèles plus récents;
- Apple TV 4K et modèles plus récents;
- Apple Watch Series 3 et modèles plus récents;
- Ordinateurs Mac (fin 2013 et modèles plus récents, avec 802.11ac ou normes ultérieures)

Les appareils plus récents prennent en charge l'authentification par protocole WPA3 Enterprise avec chiffrement 192 bits, y compris la prise en charge du chiffrement AES 256 bits lors de la connexion à des points d'accès sans fil compatibles. Cette méthode renforce davantage la protection de la confidentialité des données transmises sans fil. Le protocole WPA3 Entreprise avec chiffrement 192 bits est pris en charge sur l'iPhone 11, l'iPhone 11 Pro, l'iPhone 11 Pro Max et les appareils iOS et iPadOS plus récents.

Prise en charge de la norme PMF

En plus de protéger les données transmises sans fil, les plateformes Apple étendent les protections de niveau WPA2 et WPA3 aux trames de gestion monodiffusion et multidiffusion par le service Protected Management Frame (PMF) de la norme 802.11w. La prise en charge du PMF est offerte sur les appareils Apple suivants :

- iPhone 6 et modèles plus récents
- iPad Air 2 et modèle plus récent;
- Apple TV HD et modèles plus récents;
- Apple Watch Series 3 et modèles plus récents;
- Ordinateurs Mac (fin 2013 et modèles plus récents, avec 802.11ac ou normes ultérieures)

La prise en charge de la norme 802.1X permet aux appareils Apple de s'intégrer à un vaste éventail d'environnements d'authentification RADIUS. Les méthodes d'authentification sans fil 802.1X prises en charge comprennent EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0 et PEAPv1.

Protections des plateformes

Les systèmes d'exploitation d'Apple protègent l'appareil des vulnérabilités du programme interne du processeur réseau. Cela signifie que les contrôleurs réseau associés à la connectivité Wi-Fi ont un accès limité à la mémoire du processeur d'application.

- Lorsque le protocole USB ou SDIO (Secure Digital Input Output, entrée/sortie numérique sécurisée) est utilisé avec le processeur réseau, ce dernier ne peut pas exécuter de transactions d'accès direct en mémoire (DMA) vers le processeur d'application.
- Lorsque le protocole PCIe est utilisé, chaque processeur réseau a recours à son propre bus PCIe isolé. Une unité de gestion de la mémoire d'entrée/sortie (UGMES) sur chaque bus PCIe limite davantage le DMA du processeur réseau à la mémoire et aux ressources contenant ses paquets réseau et ses structures de contrôle.

Protocoles obsolètes

Les produits Apple prennent en charge les protocoles d'authentification Wi-Fi et de chiffrement obsolètes suivants :

- WEP Open, avec clés 40 bits et 104 bits;
- WEP Shared, avec clés 40 bits et 104 bits;
- Dynamic WEP;
- TKPI (Temporal Key Integrity Protocol);
- WPA;
- WPA/WPA2 Transitional.

Ces protocoles ne sont plus considérés comme sécurisés, et leur utilisation est fortement déconseillée pour des raisons de compatibilité, de fiabilité, de performance et de sécurité. Ils sont pris en charge à des fins de rétrocompatibilité et pourraient être retirés des versions ultérieures des logiciels.

Il est recommandé de migrer toutes les implémentations Wi-Fi vers le protocole WPA3 Personal ou WPA3 Enterprise pour offrir les connexions Wi-Fi les plus robustes, sécurisées et compatibles qui soient.

Confidentialité Wi-Fi

Distribution aléatoire des adresses MAC

Les plateformes Apple utilisent une adresse MAC (Media Access Control, contrôle d'accès au support) distribuée aléatoirement lors de la recherche de réseaux Wi-Fi jusqu'à ce qu'elles se connectent. Cette recherche peut servir à trouver un réseau Wi-Fi connu et s'y connecter, ou à aider les services de localisation qui utilisent le géorepérage, comme les rappels en fonction du lieu ou la détermination d'un emplacement dans l'app Plans d'Apple. Il convient de noter que la recherche de réseaux Wi-Fi qui se produit lors d'une tentative de connexion à un réseau connu n'est pas aléatoire. La distribution aléatoire des adresses MAC Wi-Fi est offerte sur l'iPhone 5 et les modèles plus récents.

Les plateformes Apple utilisent également une adresse MAC distribuée aléatoirement pour effectuer des recherches enhanced Preferred Network Offload (ePNO) lorsqu'un appareil n'est pas associé à un réseau Wi-Fi ou que son processeur est en veille. Ces recherches sont exécutées si un appareil fait appel aux services de localisation pour des apps utilisant le géorepérage, comme les rappels en fonction du lieu, qui déterminent si l'appareil se trouve près d'un lieu précis.

Parce que l'adresse MAC de l'appareil change quand il n'est pas connecté à un réseau Wi-Fi, elle ne peut pas être utilisée par les observateurs passifs du trafic Wi-Fi pour suivre un appareil, même s'il est connecté à un réseau cellulaire. Apple a informé les fabricants de cartes Wi-Fi que la recherche de réseaux Wi-Fi des appareils iOS et iPadOS utilise une adresse MAC distribuée aléatoirement que ni Apple ni les fabricants ne peuvent prédire.

iOS 14, iPadOS 14 et watchOS 7 comportent une nouvelle fonctionnalité de confidentialité Wi-Fi : lorsqu'un iPhone, un iPad, un iPod touch ou une Apple Watch se connecte à un réseau Wi-Fi, il s'identifie avec une adresse MAC unique (aléatoire) par réseau. Cette fonctionnalité peut être désactivée soit par l'utilisateur soit au moyen d'une nouvelle option dans l'entité Wi-Fi. Dans certaines circonstances, l'appareil aura recours à sa véritable adresse MAC.

Pour en savoir plus, consultez l'article de l'assistance Apple Utiliser des adresses Wi-Fi privées dans iOS 14, iPadOS 14 et watchOS 7.

Distribution aléatoire des numéros de séquence de trame Wi-Fi

Les trames Wi-Fi comprennent un numéro de séquence utilisé par le protocole 802.11 de bas niveau pour permettre des communications Wi-Fi fiables et efficaces. Puisque chaque trame transmise incrémente les numéros de séquence, ceux-ci pourraient être utilisés pour mettre en corrélation les informations transférées pendant les recherches de réseaux Wi-Fi avec d'autres trames transmises par le même appareil.

À titre de protection, les appareils Apple distribuent aléatoirement les numéros de séquence chaque fois qu'une adresse Mac est modifiée. Cela comprend la distribution aléatoire des numéros de séquence de chaque nouvelle demande de recherche lancée alors que l'appareil n'est pas associé. Cette fonction est prise en charge par les appareils suivants :

- iPhone 7 et modèles plus récents;
- iPad 5e génération et modèles plus récents;
- Apple TV 4K et modèles plus récents;
- Apple Watch Series 3 et modèles plus récents;
- iMac Pro (Retina 5K, 27 po, 2017) et modèles plus récents;
- MacBook Pro (13 po, 2018) et modèles plus récents;
- MacBook Pro (15 po, 2018) et modèles plus récents;
- MacBook Air (Retina, 13 po, 2018) et modèles plus récents;
- Mac mini (2018) et modèles plus récents;
- iMac (Retina 4K, 21,5 po, 2019) et modèles plus récents;
- iMac (Retina 5K, 27 po, 2019) et modèles plus récents;
- Mac Pro (2019) et modèles plus récents.

Connexions Wi-Fi

Apple génère des adresses MAC distribuées aléatoirement pour les connexions Wi-Fi pair à pair utilisées par AirDrop et AirPlay. Ces adresses sont aussi utilisées pour le partage de connexion sous iOS et iPadOS (appareils équipés d'une carte SIM) et le partage Internet sous macOS.

De nouvelles adresses distribuées aléatoirement sont générées au démarrage de ces interfaces réseau, et des adresses uniques sont générées séparément au besoin pour chaque interface.

Réseaux masqués

Les réseaux Wi-Fi sont identifiés par un *identifiant de réseau sans fil (SSID, Service Set Identifier)*, qui leur sert de nom. Certains réseaux Wi-Fi sont configurés pour masquer leur SSID, ce qui fait en sorte que le point d'accès sans fil ne diffuse pas le nom du réseau. On parle de *réseaux masqués*. Les iPhone 6s et les modèles plus récents détectent automatiquement si un réseau est masqué. L'appareil iOS ou iPadOS envoie une demande de détection contenant le SSID seulement si le réseau est masqué. Cela contribue à empêcher l'appareil de diffuser le nom des réseaux masqués auxquels il s'est déjà connecté afin de protéger davantage la confidentialité.

Sécurité Bluetooth

Les appareils Apple sont dotés de deux types de Bluetooth : Bluetooth classique et Bluetooth faible énergie (BLE). Le modèle de sécurité Bluetooth des deux versions comprend les fonctionnalités distinctes suivantes :

- *Jumelage :* processus de création d'au moins une clé secrète partagée
- *Liaison :* stockage des clés créées au cours du jumelage pour les utiliser lors des connexions subséquentes afin de former une paire d'appareils approuvés
- *Authentification :* vérification du caractère identique des clés des deux appareils
- *Chiffrement :* confidentialité des messages
- *Intégrité des messages :* protection contre la falsification des messages
- *Jumelage simple sécurisé (SSP) :* protection contre l'interception passive et les attaques de l'intercepteur

Bluetooth 4.1 a ajouté la fonctionnalité de connexions sécurisées au transport physique de Bluetooth classique (débit de base/débit accru).

Les fonctionnalités de sécurité pour chaque type de Bluetooth sont indiquées ci-dessous.

Prise en charge	Bluetooth classique	Bluetooth faible énergie
Jumelage	Courbe elliptique P-256	Algorithmes approuvés par la FIPS (AES-CMAC et courbe elliptique P-256)
Liaison	Informations sur le jumelage stockées dans un emplacement sécurisé sur les appareils iOS, iPad OS, macOS, tvOS et watchOS	Informations sur le jumelage stockées dans un emplacement sécurisé sur les appareils iOS, iPad OS, macOS, tvOS et watchOS

Prise en charge	Bluetooth classique	Bluetooth faible énergie
Authentification	Algorithmes approuvés par la FIPS (HMAC-SHA256 et AES-CTR)	Algorithmes approuvés par la FIPS
Chiffrement	Cryptographie AES-CCM réalisée dans le contrôleur	Cryptographie AES-CCM réalisée dans le contrôleur
Intégrité des messages	Mode AES-CCM utilisé pour l'intégrité des messages	Mode AES-CCM utilisé pour l'intégrité des messages
Jumelage simple sécurisé (SSP) : protection contre l'interception passive	Échange Diffie-Hellman à courbe elliptique (ECDHE)	Échange Diffie-Hellman à courbe elliptique (ECDHE)
Jumelage simple sécurisé (SSP) : protection contre les attaques de l'intercepteur	Deux méthodes numériques avec aide de l'utilisateur : comparaison numérique ou saisie d'un code d'accès	Deux méthodes numériques avec aide de l'utilisateur : comparaison numérique ou saisie d'un code d'accès Réponse de l'utilisateur requise pour les jumelages, y compris les modes sans protection contre les attaques de l'intercepteur
Bluetooth 4.1 et versions ultérieures	iMac (fin 2015) et modèles plus récents MacBook Pro (début 2015) et modèles plus récents	iOS 9 et versions ultérieures iPadOS 13.1 et versions ultérieures macOS 10.12 et versions ultérieures tvOS 9 et versions ultérieures watchOS 2.0 et versions ultérieures
Bluetooth 4.2 et versions ultérieures	iPhone 6 et modèles plus récents	iOS 9 et versions ultérieures iPadOS 13.1 et versions ultérieures macOS 10.12 et versions ultérieures tvOS 9 et versions ultérieures watchOS 2.0 et versions ultérieures

Confidentialité de Bluetooth faible énergie

Pour aider à assurer la confidentialité des utilisateurs, la technologie BLE utilise les deux fonctionnalités suivantes : la distribution aléatoire des adresses et la dérivation de clé de transport croisé.

La *distribution aléatoire des adresses* est une fonctionnalité qui réduit la capacité à suivre un appareil BLE au fil du temps en modifiant fréquemment son adresse. Pour qu'un appareil qui utilise cette fonction de confidentialité puisse se reconnecter à des appareils connus, ceux-ci doivent être en mesure de résoudre son *adresse privée*. Cette adresse privée est générée à l'aide de la clé de résolution d'identité de l'appareil qui est échangée lors du jumelage.

iOS 13, iPadOS 13.1 et les versions ultérieures de ces systèmes d'exploitation sont en mesure de dériver les clés de liaison d'une méthode de transmission à l'autre, une fonctionnalité dénommée *CTDK (Cross-Transport Key Derivation, dérivation de clé de transport croisé)*. Par exemple, une clé de liaison générée par BLE peut être utilisée pour dériver une clé de liaison Bluetooth Classic. De plus, Apple a ajouté Bluetooth classique à la prise en charge de BLE pour les appareils prenant en charge les connexions sécurisées introduites dans les spécifications principales de Bluetooth 4.1 (consultez la page Web Bluetooth Core Specification 5.1, publiée en anglais uniquement).

Sécurité de la bande ultralarge sous iOS

La puce U1, une innovation Apple, utilise une technologie à bande ultralarge pour localiser précisément l'iPhone 11, l'iPhone 11 Pro, l'iPhone 11 Pro Max et les modèles plus récents par rapport aux appareils Apple à proximité qui sont équipés de la même puce. La technologie à bande ultralarge utilise la même technologie pour la distribution aléatoire des données que les autres appareils Apple compatibles :

- Distribution aléatoire des adresses MAC
- distribution aléatoire des numéros de séquence de trame Wi-Fi.

Sécurité de l'authentification unique

Authentification unique

iOS et iPadOS prennent en charge l'authentification sur les réseaux d'entreprise par authentification unique. L'authentification unique fonctionne avec les réseaux utilisant le protocole Kerberos pour authentifier les utilisateurs auprès des services auxquels ils sont autorisés à accéder. Elle peut être utilisée pour de nombreuses activités réseau, comme l'ouverture de sessions sécurisées dans Safari et l'utilisation d'apps tierces. L'authentification par certificat comme PKINIT est également prise en charge.

macOS prend en charge l'authentification sur les réseaux d'entreprise par protocole Kerberos. Les apps peuvent faire appel à ce protocole pour authentifier les utilisateurs auprès des services qu'ils sont autorisés à utiliser. Kerberos peut aussi servir à diverses activités réseau, comme l'ouverture de sessions sécurisées dans Safari, la connexion à des systèmes de fichiers réseau et l'utilisation d'apps tierces. L'authentification par certificat est prise en charge, mais les apps doivent passer par une API de développeur.

L'authentification unique sous iOS, iPadOS et macOS fait appel à des jetons SPNEGO et au protocole HTTP Negotiate, qui sont compatibles avec les passerelles d'authentification exploitant Kerberos et avec les systèmes Integrated Windows Authentication prenant en charge les tickets Kerberos. La prise en charge de l'authentification unique repose sur le projet Heimdal en code source libre.

Les types de chiffrement suivants sont pris en charge sous iOS, iPadOS et macOS :

- AES-128-CTS-HMAC-SHA1-96;
- AES-256-CTS-HMAC-SHA1-96;
- DES3-CBC-SHA1;
- ARCFOUR-HMAC-MD5.

Safari prend en charge l'authentification unique, et les apps tierces qui utilisent les API de mise en réseau standard d'iOS et d'iPadOS peuvent également être configurées pour l'utiliser. Pour configurer l'authentification unique, iOS et iPadOS prennent en charge une entité de profil de configuration (les données utiles) qui permet aux solutions de gestion des appareils mobiles (GAM) de transmettre les réglages nécessaires. La solution de GAM peut ainsi configurer le nom de l'utilisateur principal (c'est-à-dire le compte d'utilisateur Active Directory) et les paramètres de domaine Kerberos, ainsi que la liste des apps et des URL de Safari autorisées à utiliser l'authentification unique.

Pour configurer Kerberos sous macOS, il faut obtenir des tickets avec Visualiseur de ticket, ouvrir une session dans un domaine Active Directory sous Windows ou utiliser l'outil de ligne de commande `kinit`.

Authentification unique extensible

Les développeurs d'apps peuvent implémenter leurs propres extensions d'authentification unique. Les extensions d'authentification unique sont appelées lorsqu'une app native ou une app Web doit utiliser un fournisseur d'identité pour l'authentification de l'utilisateur. Les développeurs peuvent fournir deux types d'extensions : celles qui redirigent vers HTTPS et celles qui utilisent un mécanisme défi-réponse comme Kerberos. Cela permet à l'authentification unique extensible de prendre en charge des modes d'authentification OpenID, OAuth, SAML2 et Kerberos.

Pour utiliser une extension d'authentification unique, une app peut soit utiliser l'API AuthenticationServices, soit compter sur le mécanisme d'interception URL offert par le système d'exploitation. WebKit et CFNetwork offrent une couche d'interception qui permet la prise en charge fluide de l'authentification unique pour toute app native ou WebKit. Pour qu'une extension d'authentification unique soit appelée, il faut installer une configuration fournie par un administrateur à l'aide d'un profil de gestion des appareils mobiles (GAM). En outre, les extensions de type redirection doivent utiliser les données utiles des domaines associés pour prouver que le serveur d'identité qu'elles prennent en charge est au courant de leur existence.

La seule extension d'authentification unique fournie avec le système d'exploitation est celle du protocole Kerberos.

Sécurité AirDrop

Les appareils Apple qui prennent en charge AirDrop utilisent Bluetooth faible énergie (BLE) et une technologie Wi-Fi pair à pair conçue par Apple pour envoyer des fichiers et des données aux appareils se trouvant à proximité, notamment les appareils iOS qui exécutent iOS 7 ou une version ultérieure et les ordinateurs Mac qui exécutent OS X 10.11 ou une version ultérieure, et qui sont compatibles avec AirDrop. La radio Wi-Fi permet aux appareils de communiquer directement entre eux, sans passer par une connexion Internet ou un point d'accès sans fil. Sous macOS, cette connexion est chiffrée à l'aide du protocole TLS.

Par défaut, AirDrop est configuré pour ne partager des données qu'avec les contacts. Les utilisateurs peuvent également choisir d'utiliser AirDrop pour partager des données avec tout le monde ou de désactiver complètement cette fonctionnalité. Les entreprises peuvent restreindre l'usage d'AirDrop pour les apps ou les appareils gérés par une solution de gestion des appareils mobiles (GAM).

Fonctionnement d’AirDrop

AirDrop utilise les services iCloud pour l’authentification des utilisateurs. Lorsqu’un utilisateur se connecte à iCloud, une identité RSA 2 048 bits est stockée sur l’appareil, puis lorsque l’utilisateur active AirDrop, un hachage d’identité AirDrop court est créé en fonction des adresses courriel et des numéros de téléphone associés à l’identifiant Apple de l’utilisateur.

Lorsqu’un utilisateur choisit AirDrop comme méthode de partage pour un élément, l’appareil expéditeur émet un signal AirDrop via BLE qui comprend le hachage d’identité AirDrop court de l’utilisateur. Les autres appareils Apple à proximité qui sont actifs et sur lesquels AirDrop est activé détectent le signal et répondent par l’entremise du Wi-Fi pair à pair. Ainsi, l’appareil expéditeur peut découvrir l’identité de tout appareil qui répond.

En mode Contacts uniquement, le hachage d’identité AirDrop court reçu est comparé à ceux des personnes présentes dans l’app Contacts de l’appareil destinataire. Si une correspondance est trouvée, l’appareil destinataire répond par l’entremise du Wi-Fi pair à pair avec ses informations d’identification. L’appareil ne répond pas sans correspondance.

En mode Tout le monde, le même processus général est utilisé. Cependant, l’appareil destinataire répond même s’il n’y a pas de correspondance dans son app Contacts.

L’appareil expéditeur lance ensuite une connexion AirDrop par l’entremise du Wi-Fi pair à pair pour envoyer un hachage d’identité long à l’appareil destinataire. Si le hachage d’identité long correspond à celui d’une personne connue dans les contacts de l’appareil destinataire, celui-ci répond alors avec ses hachages d’identité longs.

Si les hachages sont vérifiés, le prénom et la photo du destinataire, si disponibles dans Contacts, s’affichent dans la fiche de partage AirDrop de l’expéditeur. Sous iOS et iPadOS, ils s’affichent dans la section « Personnes » ou « Appareils ». Les appareils qui ne sont pas vérifiés ou authentifiés s’affichent dans la fiche de partage AirDrop de l’expéditeur avec une icône de silhouette et le nom de l’appareil tel qu’il a été défini dans Réglages > Général > Informations > Nom. Sous iOS et iPadOS, ils se trouvent dans la section « Autres personnes » de la fiche de partage AirDrop.

L’expéditeur peut ensuite sélectionner les utilisateurs avec qui il veut partager des données. Une fois que l’utilisateur a fait une sélection, l’appareil émetteur établit avec l’appareil récepteur une connexion chiffrée (TLS) via laquelle sont échangés les certificats d’identité iCloud. L’identité figurant dans les certificats est validée auprès de l’app Contacts de chaque utilisateur.

Si les certificats sont vérifiés, le destinataire est invité à accepter le transfert entrant en provenance de l’utilisateur ou de l’appareil identifié. Si plusieurs destinataires ont été sélectionnés, ce processus est répété pour chaque destination.

Sécurité du partage de mot de passe Wi-Fi sur iPhone et iPad

Les appareils iOS et iPadOS qui prennent en charge le partage de mot de passe Wi-Fi ont recours à un mécanisme semblable à AirDrop pour envoyer un mot de passe Wi-Fi d’un appareil à un autre.

Lorsqu'un utilisateur sélectionne un réseau Wi-Fi (demandeur) et qu'il est invité à saisir un mot de passe Wi-Fi, l'appareil Apple lance une notification Bluetooth faible énergie (BLE) indiquant qu'il souhaite obtenir le mot de passe Wi-Fi. Les autres appareils Apple à proximité qui sont actifs et qui détiennent le mot de passe du réseau Wi-Fi sélectionné se connectent à l'appareil demandeur au moyen d'une connexion BLE.

L'appareil qui détient le mot de passe Wi-Fi (cédant) exige les coordonnées du demandeur, et ce dernier doit prouver son identité à l'aide d'un mécanisme semblable à AirDrop. Une fois l'identité confirmée, le cédant envoie au demandeur le code à utiliser pour se connecter au réseau.

Les entreprises peuvent restreindre l'usage du partage de mot de passe Wi-Fi pour les apps ou les appareils gérés par une solution de gestion des appareils mobiles (GAM).

Sécurité du coupe-feu sous macOS

macOS comprend un coupe-feu intégré qui protège Mac contre les attaques réseau et les attaques par déni de service. Il peut être configuré dans la sous-fenêtre « Sécurité et confidentialité » des Préférences Système et prend en charge les configurations suivantes :

- bloquer toutes les connexions entrantes, peu importe l'app;
- autoriser automatiquement les logiciels intégrés à recevoir les connexions entrantes;
- autoriser automatiquement les logiciels signés téléchargés à recevoir les connexions entrantes;
- autoriser ou refuser l'accès à certaines apps choisies par l'utilisateur;
- empêcher le Mac de répondre aux demandes de vérification et de sondage de ports ICMP (Internet Control Message Protocol, protocole de message de contrôle sur Internet).

Sécurité de la trousse de développement

Aperçu de la sécurité de la trousse de développement

Apple fournit de nombreux cadres sous forme de « trousses » pour permettre aux développeurs tiers d'étendre les services Apple. La sécurité et la confidentialité des utilisateurs sont au cœur de ces cadres :

- HomeKit
- CloudKit
- SiriKit
- DriverKit
- ReplayKit
- ARKit

HomeKit

Sécurité de la communication HomeKit

Aperçu

HomeKit fournit une infrastructure d'automatisation à domicile qui fait appel aux fonctionnalités de sécurité d'iCloud, d'iOS, d'iPadOS et de macOS pour protéger et synchroniser les données personnelles sans les exposer à Apple.

La sécurité et l'identité HomeKit reposent sur des paires de clés publique et privée Ed25519. Une paire de clés Ed25519 est générée pour HomeKit sur l'appareil iOS, iPadOS et macOS pour chaque utilisateur et devient son identité HomeKit. Elle est utilisée pour authentifier la communication entre les appareils iOS, iPadOS et macOS, et entre les appareils iOS, iPadOS et macOS et les accessoires.

Les clés sont stockées dans le trousseau et incluses uniquement dans les sauvegardes chiffrées du trousseau. S'il y a lieu, elles sont synchronisées entre les appareils à l'aide du trousseau iCloud. Le HomePod et l'Apple TV reçoivent des clés au moyen de la fonction « Toucher pour configurer » ou du mode de configuration décrit ci-dessous. Les clés sont transmises d'un iPhone à une Apple Watch jumelée à l'aide du service d'identité d'Apple (IDS).

Communication entre les accessoires HomeKit

Les accessoires HomeKit génèrent leur propre paire de clés Ed25519 pour communiquer avec les appareils iOS, iPadOS et macOS. Si les réglages d'origine de l'accessoire sont rétablis, une nouvelle paire de clés est générée.

Pour établir une relation entre un appareil iOS, iPadOS ou macOS et un accessoire HomeKit, les clés sont échangées à l'aide du protocole Secure Remote Password (3 072 bits), en utilisant un code à 8 chiffres fourni par le fabricant de l'accessoire et saisi sur l'appareil iOS ou iPadOS par l'utilisateur, puis chiffré avec l'algorithme de chiffrement authentifié avec données associées (AEAD, Authenticated Encryption with Associated Data) ChaCha20-Poly1305 et des clés obtenues à l'aide de la fonction de dérivation HKDF-SHA512. La certification MFi de l'accessoire est également vérifiée lors de la configuration. Les accessoires sans puce MFi peuvent obtenir la prise en charge de l'authentification logicielle sous iOS 11.3 et les versions ultérieures.

Lorsque l'appareil iOS, iPadOS ou macOS et l'accessoire HomeKit communiquent, chacun authentifie l'autre en utilisant les clés échangées de la façon décrite ci-dessus. Chaque session est établie à l'aide du protocole Station-to-Station et chiffrée avec les clés obtenues avec la fonction de dérivation HKDF-SHA512 à partir des clés Curve25519 de session. Cela s'applique aux accessoires IP et aux accessoires Bluetooth faible énergie (BLE).

Pour les appareils BLE qui prennent en charge les notifications de diffusion, l'accessoire reçoit une clé de chiffrement de diffusion de la part d'un appareil iOS, iPadOS ou macOS jumelé au cours d'une session sécurisée. Cette clé est utilisée pour chiffrer les données concernant les changements d'état de l'accessoire, qui sont signalés par les notifications BLE. La clé de chiffrement de diffusion est une clé obtenue à l'aide de la fonction de dérivation HKDF-SHA512, et les données sont chiffrées avec l'algorithme AEAD ChaCha20-Poly1305. La clé de chiffrement de diffusion est régulièrement modifiée par l'appareil iOS, iPadOS ou macOS et synchronisée avec les autres appareils à l'aide d'iCloud, comme le décrit la section Sécurité des données HomeKit.

HomeKit et Siri

Siri peut être utilisé pour interroger et commander les accessoires, et pour activer des scènes. Un minimum d'informations sur la configuration du domicile est donné de façon anonyme à Siri afin de communiquer le nom des pièces, des accessoires et des scènes nécessaires à la reconnaissance des commandes. Il se peut que le contenu audio envoyé à Siri fasse état d'accessoires ou de commandes spécifiques, mais ces données de Siri ne sont pas associées aux autres fonctionnalités d'Apple comme HomeKit.

Sécurité des données HomeKit

Synchronisation des données HomeKit entre les appareils et les utilisateurs

Les données HomeKit peuvent être synchronisées entre les appareils iOS, iPadOS et macOS d'un utilisateur à l'aide d'iCloud et du trousseau iCloud. Au cours de ce processus, les données HomeKit sont chiffrées au moyen de clés dérivées de l'identité HomeKit de l'utilisateur et d'un nonce aléatoire. Elles sont traitées sous forme de grand objet binaire, ou *BLOB*, opaque. Le BLOB le plus récent est stocké dans iCloud, mais il n'est pas utilisé à d'autres fins. Comme il est chiffré à l'aide de clés disponibles uniquement sur les appareils iOS, iPadOS et macOS de l'utilisateur, son contenu est inaccessible pendant la transmission et le stockage sur iCloud.

Les données HomeKit sont également synchronisées entre plusieurs utilisateurs du même domicile. Ce processus fait appel à une authentification et à un chiffrement identiques à ceux utilisés entre un appareil iOS, iPadOS ou macOS et un accessoire HomeKit. L'authentification est basée sur des clés publiques Ed25519 échangées entre les appareils lorsqu'un utilisateur est ajouté à un domicile. Après l'ajout d'un utilisateur à un domicile, toutes les communications ultérieures sont authentifiées et chiffrées à l'aide du protocole STS (Station-to-Station) et des clés de session.

L'utilisateur ayant initialement créé le domicile dans HomeKit ou tout autre utilisateur autorisé à apporter des modifications peuvent ajouter des utilisateurs. Les accessoires sont configurés sur l'appareil du propriétaire avec la clé publique du nouvel utilisateur, de sorte qu'ils pourront authentifier et accepter les commandes de cet utilisateur. Lorsqu'un utilisateur autorisé à apporter des modifications ajoute un nouvel utilisateur, le processus est délégué à un concentrateur pour conclure l'opération.

La configuration de l'Apple TV avec HomeKit est automatique lorsque l'utilisateur se connecte à iCloud. L'authentification à deux facteurs doit être activée sur le compte iCloud. L'Apple TV et l'appareil du propriétaire échangent temporairement les clés publiques Ed25519 via iCloud. Si l'appareil du propriétaire et l'Apple TV sont connectés au même réseau local, les clés temporaires sont utilisées pour sécuriser une connexion sur le réseau local à l'aide du protocole STS et des clés de session. Ce processus fait appel à une authentification et à un chiffrement identiques à ceux utilisés entre un appareil iOS, iPadOS ou macOS et un accessoire HomeKit. L'appareil du propriétaire transfère les paires de clés publique et privée Ed25519 vers l'Apple TV via cette connexion locale sécurisée. Ces clés sont ensuite utilisées pour sécuriser la communication entre l'Apple TV et les accessoires HomeKit, ainsi qu'entre l'Apple TV et les autres appareils iOS, iPadOS et macOS du domicile HomeKit.

Si l'utilisateur n'a qu'un seul appareil et qu'il n'accorde pas l'accès à son domicile à d'autres utilisateurs, aucune donnée HomeKit n'est transmise à iCloud.

Données du domicile et apps

L'accès des apps aux données du domicile est contrôlé par les réglages de confidentialité de l'utilisateur. Lorsque des apps demandent à accéder aux données du domicile, l'utilisateur est invité à indiquer son choix, comme pour Contacts, Photos et d'autres sources de données iOS, iPadOS et macOS. S'il donne son accord, les apps peuvent connaître les noms des pièces et des accessoires, savoir dans quelle pièce se trouve chaque accessoire et accéder à d'autres informations, comme l'indique en détail la documentation du développeur HomeKit à l'adresse https://developer.apple.com/homekit/.

Stockage local des données

HomeKit stocke les données concernant les domiciles, les accessoires, les scènes et les utilisateurs sur les appareils iOS, iPadOS ou macOS d'un utilisateur. Ces données stockées sont chiffrées à l'aide de clés obtenues à partir des clés de l'identité HomeKit de l'utilisateur et d'un nonce aléatoire. En outre, les données HomeKit sont stockées avec la classe de protection des données « Protection complète jusqu'à la première authentification de l'utilisateur ». Les données HomeKit sont sauvegardées uniquement dans les sauvegardes chiffrées. Par exemple, les sauvegardes non chiffrées effectuées avec le Finder (sous macOS 10.15 ou version ultérieure) ou iTunes (sous macOS 10.14 ou version antérieure) au moyen d'une connexion USB ne contiennent donc pas de données HomeKit.

Sécurisation des routeurs avec HomeKit

Les routeurs qui prennent en charge HomeKit permettent aux utilisateurs d'améliorer la sécurité de leur réseau domestique en gérant l'accès Wi-Fi des accessoires HomeKit à leur réseau local et à Internet. Les routeurs prennent aussi en charge l'authentification PSK personnelle (PPSK) de façon à ce que chaque accessoire puisse être ajouté au réseau Wi-Fi à l'aide d'une clé qui lui est propre et qui est révocable au besoin. L'authentification PPSK améliore la sécurité, car le mot de passe Wi-Fi principal n'est pas divulgué aux accessoires, et le routeur peut les identifier de manière sécurisée même s'ils changent d'adresse MAC.

Dans l'app Domicile, un utilisateur peut configurer des restrictions d'accès pour les groupes d'accessoires :

- *Aucune restriction :* Ce réglage donne un accès non restreint à Internet et au réseau local.
- *Automatique :* Il s'agit du réglage par défaut. Celui-ci donne accès à Internet et au réseau local selon une liste de sites Internet et de ports locaux fournie à Apple par le fabricant de l'accessoire. Cette liste comprend tous les sites et ports dont l'accessoire a besoin pour fonctionner correctement. (Le réglage « Aucune restriction » est en place jusqu'à ce que cette liste soit disponible.)
- *Limiter au domicile :* Aucun accès à Internet ni au réseau local, sauf pour les connexions requises par HomeKit pour trouver et contrôler l'accessoire depuis le réseau local (y compris à partir du concentrateur pour prendre en charge la commande à distance).

La clé PPSK est une phrase secrète robuste de type WPA2 Personal propre à l'accessoire qui est automatiquement générée par HomeKit et révoquée lorsque l'accessoire est supprimé du domicile. Une clé PPSK est utilisée lorsqu'un accessoire est ajouté au réseau Wi-Fi par HomeKit dans un domicile configuré avec un routeur HomeKit. Ce cas de figure est reconnaissable par les données d'identification Wi-Fi « Gérées par HomeKit » à l'écran des réglages de l'accessoire dans l'app Domicile. Les accessoires qui ont été ajoutés au réseau Wi-Fi avant l'ajout du routeur sont reconfigurés pour utiliser une PPSK si l'accessoire prend en charge ce type de clé, sinon ils conservent leurs informations d'identification actuelles.

Comme mesure de sécurité supplémentaire, les utilisateurs doivent configurer le routeur HomeKit à l'aide de l'app fournie par le fabricant afin que celle-ci puisse confirmer que les utilisateurs ont accès au routeur et qu'ils peuvent l'ajouter à l'app Domicile.

Sécurité des caméras HomeKit

Les caméras qui ont une adresse IP (Internet Protocol, protocole Internet) dans HomeKit envoient des flux vidéo et audio directement à l'appareil iOS, iPadOS, tvOS ou macOS connecté au réseau local y ayant accès. Les flux sont chiffrés à l'aide de clés générées aléatoirement sur l'appareil et sur la caméra réseau (ou caméra IP), qui sont échangées au moyen de la session HomeKit sécurisée donnant accès à la caméra. Lorsqu'un appareil n'est pas connecté au réseau local, les flux chiffrés lui sont relayés par le concentrateur. Le concentrateur ne déchiffre pas les flux. Il sert simplement de relais entre l'appareil et la caméra réseau. Lorsqu'une app affiche l'image vidéo de la caméra réseau HomeKit à l'attention de l'utilisateur, HomeKit assure sa conversion sécurisée à partir d'un processus système séparé. Ainsi, l'app n'est pas en mesure d'accéder au flux vidéo ou de le stocker. En outre, les apps ne sont pas autorisées à saisir des captures d'écran de ce flux.

Vidéo sécurisée HomeKit

HomeKit offre un mécanisme sécurisé et privé de bout en bout pour enregistrer, analyser et visionner des clips filmés par les caméras réseau HomeKit sans les exposer à Apple ou à un tiers. Lorsque la caméra réseau détecte des mouvements, elle envoie des vidéoclips directement à l'appareil Apple qui sert de concentrateur, à l'aide d'une connexion réseau locale établie entre ce concentrateur et la caméra réseau. Cette connexion dédiée est chiffrée avec une paire de clés de session obtenue par la fonction de dérivation HKDF-SHA512, qui est négociée au cours de la session HomeKit entre le concentrateur et la caméra réseau. HomeKit déchiffre les flux audio et vidéo sur le concentrateur et analyse localement les images vidéo pour déceler des événements importants. En cas de détection d'un événement important, HomeKit chiffre le vidéoclip à l'aide de l'algorithme AES-256-GCM avec une clé AES256 générée aléatoirement. HomeKit génère aussi des cadres d'affiche pour chaque clip et les chiffre à l'aide de la même clé AES256. Une fois chiffrés, le cadre d'affiche ainsi que les données audio et vidéo sont téléchargés vers les serveurs iCloud. Les métadonnées associées à chaque clip ainsi que la clé de chiffrement sont téléchargées vers CloudKit à l'aide du chiffrement iCloud de bout en bout.

Pour la classification des visages, HomeKit stocke toutes les données utilisées pour classer le visage d'une personne dans CloudKit au moyen d'un chiffrement de bout en bout iCloud. Les données stockées comprennent des informations sur chaque personne, comme son nom et des images qui représentent son visage. Ces images de visages peuvent provenir de l'app Photos d'un utilisateur, s'il en décide ainsi, ou elles peuvent être extraites de vidéos prises par la caméra réseau qui ont déjà été analysées. Une session d'analyse de la vidéo sécurisée HomeKit utilise ces données de classification pour identifier les visages dans le flux vidéo sécurisé de la caméra réseau. Elle inclut ces informations d'identification dans les métadonnées du vidéoclip mentionnées précédemment.

Lorsque l'app Domicile est utilisée pour afficher les clips d'une caméra, les données sont téléchargées à partir d'iCloud, et les clés nécessaires au déchiffrement des flux sont débloquées localement à l'aide du déchiffrement iCloud de bout en bout. Le contenu vidéo chiffré est diffusé à partir des serveurs et déchiffré localement sur l'appareil iOS avant d'être affiché dans le visualiseur. Chaque session du vidéoclip peut être divisée en sous-sections dont chacune chiffre le flux de contenu à l'aide de sa propre clé unique.

Sécurité de HomeKit avec avec l'Apple TV

Utilisation d'accessoires de télécommande tiers avec l'Apple TV

Certains accessoires de télécommande tiers transmettent des événements HID (Human Interface Design, conception d'interfaces humaines) et des données audio de Siri à une Apple TV associée par l'entremise de l'app Domicile. La télécommande envoie les événements HID par l'entremise de la session sécurisée à l'Apple TV. Une télécommande compatible avec Siri envoie des données audio à l'Apple TV lorsque l'utilisateur active explicitement le microphone de la télécommande à l'aide d'un bouton dédié à Siri. La télécommande envoie les pistes audio directement à l'Apple TV au moyen d'une connexion dédiée sur le réseau local. Une paire de clés de session obtenue par la fonction de dérivation HKDF-SHA512, qui est négociée au cours de la session HomeKit entre l'Apple TV et la télécommande, est utilisée pour chiffrer la connexion au réseau local. HomeKit déchiffre les pistes audio sur l'Apple TV et les transmet à l'app Siri, où elles sont traitées selon les mêmes protections de confidentialité que toutes les entrées audio de Siri.

Profils Apple TV pour les domiciles HomeKit

Lorsqu'un utilisateur d'un domicile HomeKit ajoute son profil à l'Apple TV du propriétaire du domicile, cela lui donne accès à ses émissions de télévision, à sa musique et à ses balados. Les réglages de chaque utilisateur concernant l'utilisation de son profil sur l'Apple TV sont partagés avec le compte iCloud du propriétaire à l'aide du chiffrement de bout en bout. Les données appartiennent à chaque utilisateur et sont partagées avec le propriétaire en lecture seule. Chaque utilisateur du domicile peut modifier ces valeurs dans l'app Domicile, et l'Apple TV du propriétaire utilise ces réglages.

Lorsqu'un réglage est activé, le compte iTunes de l'utilisateur devient disponible sur l'Apple TV. Lorsqu'un réglage est désactivé, les comptes et les données de cet utilisateur sont supprimés de l'Apple TV. Le partage CloudKit initial est lancé par l'appareil de l'utilisateur, et le jeton servant à sécuriser ce partage est envoyé par le même canal sécurisé que celui utilisé pour la synchronisation des données entre les utilisateurs du domicile.

Accessoires HomeKit et iCloud

Remarque : Dans la mesure du possible, accédez aux services par l'entremise directe d'un concentrateur plutôt que par iCloud. Par exemple, utilisez un concentrateur, comme un HomePod, une Apple TV ou un iPad.

L'accès distant à iCloud est toujours pris en charge pour les appareils HomeKit plus anciens. Apple a conçu ces appareils avec soin pour que les utilisateurs puissent les contrôler et leur envoyer des notifications sans divulguer à Apple l'identité des accessoires ou la nature des commandes et des notifications envoyées. HomeKit n'envoie jamais d'informations relatives au domicile au moyen de l'accès distant à iCloud.

Authentification mutuelle d'un accessoire et d'un appareil Apple

Lorsqu'un utilisateur envoie une commande par l'intermédiaire de l'accès distant à iCloud, l'accessoire et l'appareil iOS, iPadOS ou macOS sont mutuellement authentifiés et les données sont chiffrées en utilisant la même procédure que celle décrite pour les connexions locales. Le contenu des transmissions est chiffré et n'est pas divulgué à Apple. L'adressage à travers iCloud s'articule autour d'identifiants iCloud inscrits au cours du processus de configuration.

Processus de configuration des accessoires

Les accessoires prenant en charge l'accès distant à iCloud sont attribués pendant le processus de configuration de l'accessoire. Le processus d'attribution commence par la connexion de l'utilisateur à iCloud. L'appareil iOS ou iPadOS demande ensuite à l'accessoire de signer un défi en utilisant le coprocesseur d'authentification d'Apple, intégré à tous les accessoires conçus pour HomeKit. L'accessoire génère également des clés à partir de la courbe elliptique prime256v1, et la clé publique est envoyée à l'appareil iOS ou iPadOS accompagnée du défi signé et du certificat X.509 du coprocesseur d'authentification. Ceux-ci servent à demander un certificat pour l'accessoire à partir du serveur d'attribution iCloud. Le certificat est stocké par l'accessoire, mais il ne contient aucune information d'identification sur l'accessoire, hormis la mention que l'accès distant à iCloud pour HomeKit lui a été accordé. L'appareil iOS ou iPadOS conduisant l'attribution envoie également un conteneur à l'accessoire, incluant les URL et d'autres informations nécessaires pour la connexion au serveur d'accès à distance iCloud. Ces informations ne sont pas spécifiques à un utilisateur ni à un accessoire en particulier.

Liste des utilisateurs autorisés d'un accessoire

Chaque accessoire inscrit une liste d'utilisateurs autorisés auprès du serveur d'accès à distance iCloud. Ces utilisateurs ont obtenu de l'utilisateur ayant ajouté l'accessoire au domicile la permission de contrôler l'accessoire. Le serveur iCloud attribue aux utilisateurs un identifiant qui peut être mis en correspondance avec un compte iCloud dans le but de distribuer les messages de notification et les réponses des accessoires. De même, les accessoires possèdent un identifiant fourni par iCloud, mais qui est opaque et ne révèle aucune information relative à l'accessoire même.

Connexion des accessoires au serveur d'accès à distance iCloud

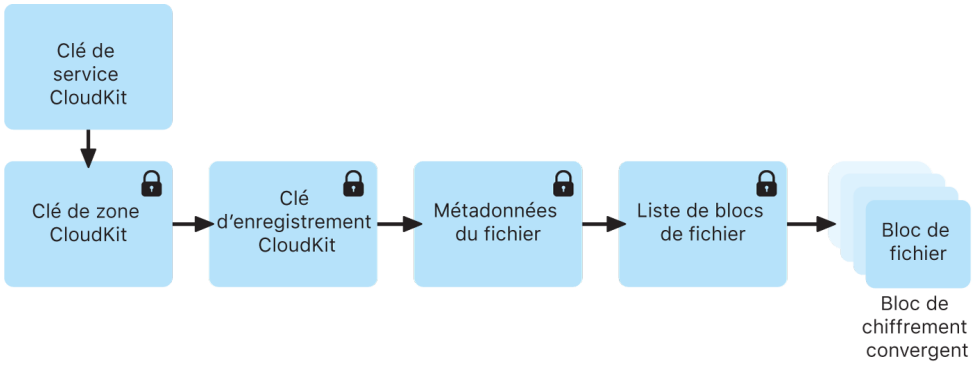
Lorsqu'un accessoire se connecte au serveur d'accès à distance iCloud pour HomeKit, il présente son certificat et un billet. Ce billet, qui est obtenu auprès d'un serveur iCloud différent, n'est pas propre à chaque accessoire. Lorsqu'un accessoire demande un billet, il indique dans sa requête son fabricant, son modèle et la version de son programme interne. Aucune information d'identification de l'utilisateur ou du domicile n'est envoyée dans cette requête. Pour protéger la confidentialité, la connexion au serveur de billet n'est pas authentifiée.

Les accessoires se connectent au serveur d'accès à distance iCloud par HTTP/2, dont la liaison est sécurisée par TLS 1.2 avec AES128-GCM et SHA256. L'accessoire garde sa connexion au serveur d'accès à distance iCloud ouverte afin de pouvoir recevoir les messages entrants ainsi qu'envoyer les réponses et les notifications sortantes aux appareils iOS, iPadOS et macOS.

Sécurité de CloudKit

CloudKit est un cadre d'application qui permet aux développeurs d'apps d'enregistrer des données clé-valeur, des données structurées et des ressources dans iCloud. L'accès à CloudKit est contrôlé au moyen de déclarations d'autorisation d'app. CloudKit prend en charge les bases de données publiques et privées. Les bases de données publiques sont utilisées par toutes les instances de l'app, habituellement pour des ressources générales, et ne sont pas chiffrées. Les bases de données privées hébergent les données de l'utilisateur.

Comme avec iCloud Drive, CloudKit utilise des clés basées sur le compte pour protéger les informations stockées dans la base de données privée de l'utilisateur et, comme pour d'autres services iCloud, les fichiers sont divisés en blocs, chiffrés et stockés par l'entremise de services tiers. CloudKit utilise une hiérarchie de clés comme pour la protection des données. Les clés par fichier sont enveloppées par des clés d'enregistrement CloudKit. Ces dernières sont à leur tour protégées par une clé de zone, elle-même protégée par la clé de service CloudKit de l'utilisateur. La clé de service CloudKit est stockée dans le compte iCloud de l'utilisateur et n'est disponible qu'une fois que ce dernier s'est authentifié sur iCloud.



Chiffrement de bout en bout CloudKit.

Sécurité de SiriKit pour iOS, iPadOS et watchOS

Siri utilise le système d'extension d'app pour communiquer avec les apps tierces. Sur un appareil, Siri peut accéder directement aux contacts de l'utilisateur et à la position de l'appareil. Cependant, avant de fournir des données protégées à une app, Siri vérifie les autorisations d'accès de l'app contrôlées par l'utilisateur. En fonction de ces autorisations, Siri ne transmet que le fragment pertinent de la demande d'origine de l'utilisateur à l'extension d'app. Par exemple, si une app n'a pas accès aux contacts, Siri ne pourra pas comprendre la relation mentionnée dans les demandes d'utilisateur comme « Envoie 10 $ à ma mère avec l'app de paiement ». Dans ce cas, l'app ne verrait que le terme littéral « ma mère ».

Cependant, si l'utilisateur a donné à l'app accès aux contacts, l'app recevra les informations interprétées au sujet de la mère de l'utilisateur. Si une relation est mentionnée dans le corps d'un message, par exemple « Dis à ma mère sur l'app de messagerie que mon frère est génial », Siri n'interprétera pas « mon frère », quelles que soient les modalités de l'app.

Les apps compatibles avec SiriKit peuvent envoyer à Siri du vocabulaire propre à l'app ou à l'utilisateur, comme le nom des contacts de l'utilisateur. Ces informations permettent à la reconnaissance vocale et à la compréhension du langage naturel de Siri de reconnaître le vocabulaire de cette app et elles sont associées à un identifiant aléatoire. Les informations personnalisées demeurent disponibles tant que l'identifiant est utilisé, jusqu'à ce que l'utilisateur désactive l'intégration de Siri pour cette app dans Réglages ou jusqu'à ce que l'app compatible avec SiriKit soit désinstallée.

Pour une demande comme « Obtiens un trajet jusque chez ma mère avec l'app de covoiturage », la demande requiert les données de localisation des contacts de l'utilisateur. Uniquement pour cette demande, Siri fournit les informations nécessaires à l'extension d'app, peu importe les réglages d'autorisation de l'utilisateur concernant la localisation ou les contacts.

Sécurité de DriverKit pour macOS 10.15

DriverKit est le cadre d'application qui permet aux développeurs de créer des pilotes de périphérique que l'utilisateur installe sur son Mac. Les pilotes conçus avec DriverKit s'exécutent dans l'espace utilisateur plutôt qu'en tant qu'extensions du noyau, ce qui améliore la sécurité et la stabilité du système. Cela facilite l'installation tout en renforçant la stabilité et la sécurité de macOS.

L'utilisateur n'a qu'à télécharger l'app (aucun programme d'installation n'est requis avec les extensions système ou DriverKit), et l'extension est activée seulement lorsque nécessaire. Dans plusieurs cas, cela évite d'utiliser des extensions de noyau dont l'installation dans /System/Library or /Library nécessite des privilèges d'administrateur.

Nous conseillons aux administrateurs de TI qui utilisent des pilotes de périphérique, des solutions de stockage infonuagique, des réseaux ou des apps de sécurité qui requièrent des extensions de noyau de passer à des versions plus récentes dotées d'extensions système. Ces versions plus récentes réduisent grandement les risques d'erreurs graves du noyau sur Mac, mais aussi la surface d'attaque. Les nouvelles extensions, qui s'exécutent dans l'environnement utilisateur, ne requièrent aucun privilège pour leur installation et sont automatiquement retirées lorsque le groupe d'apps est placé dans la corbeille.

Le cadre DriverKit offre des classes C++ pour les services entrée/sortie, la correspondance d'appareils, les descripteurs de mémoire et les files de transmission. Il définit également les types d'entrée/sortie appropriés pour les numéros, les collectes, les chaînes et d'autres types communs. L'utilisateur s'en sert avec les cadres de pilotes propres à la famille comme USBDriverKit et HIDDriverKit. Utilisez le cadre d'application Extensions système pour installer et mettre à niveau un pilote.

Sécurité de ReplayKit pour iOS et iPadOS

ReplayKit est un cadre d'application bêta qui permet aux développeurs d'ajouter aux apps des fonctionnalités d'enregistrement et de diffusion en direct. De plus, il permet aux utilisateurs d'annoter les enregistrements et les diffusions à l'aide de la caméra avant et du micro de l'appareil.

Enregistrement vidéo

L'enregistrement d'une vidéo comprend plusieurs couches de sécurité :

- *Boîte de dialogue Autorisations :* Avant de démarrer l'enregistrement, ReplayKit demande à l'utilisateur, au moyen d'une alerte de consentement, de confirmer son intention d'enregistrer l'écran et les contenus capturés par le micro et la caméra avant. Cette alerte est présentée une fois par processus d'app et présentée à nouveau si l'app est mise en arrière-plan pendant plus de huit minutes.
- *Captures d'écran et audio :* Les captures d'écran et audio ont lieu en dehors du processus de l'app dans le démon replayd de ReplayKit, ce qui vise à garantir que le contenu enregistré n'est jamais accessible au processus de l'app.
- *Captures d'écran et audio dans l'app :* Elles permettent à une app d'obtenir des tampons vidéo et d'échantillons, qui sont protégés par la boîte de dialogue des autorisations.
- *Création et stockage de vidéos :* Le fichier vidéo est écrit dans un répertoire qui est seulement accessible aux sous-systèmes de ReplayKit et n'est jamais accessible aux apps. Cela contribue à empêcher l'utilisation des enregistrements par des tiers sans le consentement de l'utilisateur.
- *Prévisualisation et partage par l'utilisateur final :* L'utilisateur peut prévisualiser et partager la vidéo avec l'interface utilisateur promue par ReplayKit. L'interface utilisateur est présentée en dehors du processus au moyen de l'infrastructure des extensions iOS et a accès au fichier vidéo généré.

Diffusion ReplayKit

La diffusion d'une vidéo comprend plusieurs couches de sécurité :

- *Captures d'écran et audio :* Le mécanisme de capture d'écran et audio pendant la diffusion est identique à l'enregistrement de vidéos et a lieu dans `replayd`.
- *Extensions de diffusion :* Pour pouvoir participer à la diffusion ReplayKit, les services de tiers doivent créer deux nouvelles extensions qui sont configurées à l'aide du terminal com.apple.broadcast-services :
    - une extension d'interface utilisateur qui permet à l'utilisateur de configurer sa diffusion;

- une extension de téléchargement qui permet de télécharger les données vidéo et audio vers les serveurs principaux du service.

L'architecture contribue à garantir que les apps hôtes ne bénéficient d'aucun privilège sur le contenu audiovisuel diffusé. Seuls ReplayKit et les extensions de diffusion tierces y ont accès.

- *Sélecteur de diffusion :* Cette fonction permet à l'utilisateur de lancer des diffusions du système directement depuis l'app à l'aide de la même interface utilisateur que celle définie par le système, qui est accessible à partir du centre de contrôle. L'interface utilisateur est implémentée à l'aide d'une API privée et réside sous forme d'extension dans le cadre d'application de ReplayKit. Cette fonction se trouve en dehors du processus de l'app hôte.
- *Extension de téléchargement :* L'extension que les services de diffusion tiers implémentent pour traiter le contenu audiovisuel pendant la diffusion utilise des tampons d'échantillon bruts non codés. Lorsque ce mode de traitement est appliqué, les données vidéo et audio sont sérialisées et transmises en temps réel à l'extension de téléchargement tierce au moyen d'une connexion XPC directe. Les données vidéo sont codées en extrayant l'objet IOSurface du tampon d'échantillon de la vidéo, en les codant de façon sécurisée comme objet XPC, en les envoyant à l'extension tierce au moyen de la connexion XPC et en les décodant de façon sécurisée dans un objet IOSurface.

Sécurité d'ARKit pour iOS et iPadOS

ARKit est un cadre d'application qui permet aux développeurs de produire des expériences de réalité augmentée dans leurs apps ou leurs jeux. Les développeurs peuvent ajouter des éléments en 2D ou en 3D au moyen de la caméra avant ou arrière d'un appareil iOS ou iPadOS.

Apple a conçu ses caméras en tenant compte de la confidentialité, et les apps tierces doivent obtenir le consentement de l'utilisateur avant d'y accéder. Sous iOS et iPadOS, lorsqu'un utilisateur autorise une app à accéder aux caméras, l'app peut accéder à des images en temps réel provenant des caméras avant et arrière. Les apps ne sont pas autorisées à utiliser les caméras sans l'indiquer à l'utilisateur.

Les photos et les vidéos prises avec la caméra peuvent contenir d'autres informations telles que l'endroit et le moment où elles sont prises, la profondeur du champ et la capture hors champ. Si les utilisateurs ne veulent pas que les photos et vidéos prises avec l'app Appareil photo soient accompagnées des données de localisation, ils peuvent modifier ce réglage à tout moment dans Réglages > Confidentialité > Service de localisation > Appareil photo. Si les utilisateurs ne veulent pas que les photos et vidéos soient accompagnées des données de localisation lorsqu'elles sont partagées, ils peuvent désactiver la localisation dans le menu Options de la fiche de partage.

Afin de mieux positionner l'expérience de réalité augmentée de l'utilisateur, les apps qui utilisent ARKit peuvent recourir aux données de détection de l'environnement et de détection du visage de l'autre caméra. La détection de l'environnement fait appel aux algorithmes sur l'appareil de l'utilisateur pour traiter les informations provenant des capteurs et déterminer sa position dans un espace réel. La détection de l'environnement soutient des fonctionnalités telles que la direction optique dans Plans.

Gestion sécurisée des appareils

Aperçu de la gestion sécurisée des appareils

iOS, iPadOS, macOS et tvOS prennent en charge des règlements de sécurité et des options de configuration souples et faciles à appliquer et à gérer. Grâce à eux, les organisations peuvent protéger leurs données et aider à garantir que les employés respectent leurs exigences, même s'ils utilisent leurs propres appareils (dans le cadre d'un programme « Apportez votre appareil », par exemple).

Les organisations peuvent recourir à des outils comme la protection par mot de passe, les profils de configuration, l'effacement à distance et les solutions de gestion des appareils mobiles (GAM) de tiers pour gérer leurs parcs d'appareils et protéger leurs données, même lorsque les employés accèdent à celles-ci sur leurs propres appareils.

Sous iOS 13, iPadOS 13.1, macOS 10.15 et les versions ultérieures de ces systèmes d'exploitation, les appareils Apple proposent une nouvelle fonctionnalité d'inscription par l'utilisateur spécialement conçue pour les programmes du type « Apportez votre appareil ». Les utilisateurs ont ainsi une plus grande autonomie et les données de l'organisation sont mieux protégées puisqu'elles sont stockées sur un volume APFS (système de fichiers d'Apple) chiffré distinct. La sécurité, la protection de la vie privée et l'expérience des utilisateurs dans le cadre des programmes du type « Apportez votre appareil » s'en trouvent donc améliorées.

Sécurité du modèle de jumelage pour iPhone et iPad

iOS et iPadOS utilisent un modèle de jumelage pour contrôler l'accès à un appareil à partir d'un ordinateur hôte. Le jumelage établit une relation de confiance entre l'appareil et son hôte connecté, concrétisée par un échange de clés publiques. iOS et iPadOS utilisent également cette marque de confiance pour activer des fonctionnalités supplémentaires avec l'hôte connecté, comme la synchronisation de données. Sous iOS 9 et les versions ultérieures, les services :

- qui nécessitent un jumelage ne peuvent pas être lancés tant que l'appareil n'a pas été déverrouillé par l'utilisateur;
- ne démarreront pas à moins que l'appareil ait été déverrouillé récemment;
- (comme la synchronisation de photos) peuvent nécessiter le déverrouillage de l'appareil avant de commencer.

Le processus de jumelage nécessite que l'utilisateur déverrouille l'appareil et accepte la demande de jumelage envoyée par l'hôte. Sous iOS 9 et les versions ultérieures, l'utilisateur doit également saisir son code pour que l'hôte et l'appareil échangent et enregistrent les clés publiques RSA 2 048 bits. L'hôte reçoit ensuite une clé 256 bits qui peut déverrouiller le conteneur de clés de l'autorité de séquestre stocké sur l'appareil. Les clés échangées sont utilisées pour lancer une session SSL chiffrée, nécessaire pour que l'appareil puisse envoyer des données protégées à l'hôte ou démarrer un service (synchronisation avec iTunes ou le Finder, transfert de fichiers, développement Xcode, etc.). Afin d'utiliser cette session chiffrée pour toutes les communications, l'appareil nécessite des connexions d'un hôte par Wi-Fi. Il doit donc avoir déjà été jumelé par USB. Le jumelage permet aussi d'activer plusieurs fonctionnalités de diagnostic. Sous iOS 9, si la fiche d'un jumelage n'a pas été utilisée pendant plus de six mois, elle expire. Sous iOS 11 et les versions ultérieures, ce délai est réduit à 30 jours.

Certains services de diagnostic, comme com.apple.mobile.pcapd, ne peuvent fonctionner qu'au moyen d'une connexion USB. De même, le service com.apple.file_relay requiert un profil de configuration signé par Apple pour être installé. Sous iOS 11 et les versions ultérieures, l'Apple TV peut avoir recours au protocole Secure Remote Password (SRP) afin d'établir un jumelage sans fil.

L'utilisateur peut effacer la liste des hôtes fiables à l'aide des options « Réinitialiser les réglages réseau » ou « Réinitialiser localisation et confidentialité ».

Gestion des appareils mobiles

Aperçu de la sécurité de la gestion des appareils mobiles

Aperçu

La prise en charge de la gestion des appareils mobiles (GAM) par les systèmes d'exploitation Apple permet aux entreprises de configurer et de gérer en toute sécurité des déploiements d'appareils Apple à grande échelle. Les fonctionnalités de GAM exploitent les technologies des systèmes d'exploitation existantes, comme les profils de configuration, l'inscription sans fil et le service de notifications Push d'Apple (APN). Par exemple, le service APN sert à activer l'appareil pour qu'il puisse communiquer directement avec la solution de GAM par connexion sécurisée. Avec le service APN, aucun renseignement d'identification ni aucune donnée confidentielle ne sont transmis.

Avec la GAM, les services des TI peuvent inscrire des appareils Apple à l'environnement de l'entreprise, en configurer et mettre à jour les réglages à distance, vérifier le respect des politiques, gérer les mises à jour logicielles, et même verrouiller ou effacer à distance les appareils gérés.

En plus des modes d'inscription des appareils traditionnels pris en charge par iOS, iPadOS, macOS et tvOS, un type d'inscription a été ajouté sous iOS 13, iPadOS 13.1, macOS 10.15 et les versions ultérieures de ces systèmes d'exploitation : l'inscription par l'utilisateur. L'inscription par l'utilisateur est un mode d'inscription à la GAM qui vise spécifiquement les déploiements « Apportez votre appareil », dans le cadre desquels un appareil appartenant à l'employé est utilisé dans un environnement géré. L'inscription par l'utilisateur accorde à la solution de GAM des privilèges plus limités par rapport à l'inscription d'appareils non supervisés et fournit une séparation chiffrée entre l'utilisateur et les données de l'entreprise.

Types d’inscription

- *Inscription par l’utilisateur :* L’inscription par l’utilisateur est conçue pour les appareils personnels. Elle est intégrée à l’identifiant Apple géré pour définir l’identité d’un utilisateur sur un appareil. L’identifiant Apple géré est lié au profil d’inscription par l’utilisateur, et l’utilisateur doit s’authentifier avec succès pour pouvoir terminer l’inscription. L’identifiant Apple géré peut être utilisé de pair avec l’identifiant Apple personnel dont l’utilisateur s’est servi pour se connecter. Les apps et les comptes gérés utilisent un identifiant Apple géré tandis que les apps et les comptes personnels utilisent un identifiant Apple personnel.
- *Inscription des appareils :* L’inscription des appareils permet aux organisations de demander aux utilisateurs d’inscrire manuellement des appareils et de gérer différents aspects de leur utilisation, y compris la capacité à effacer l’appareil. L’inscription des appareils offre également un ensemble plus vaste d’entités et de restrictions applicables aux appareils. Lors qu’un utilisateur supprime un profil d’inscription, tous les profils de configuration, les réglages et les apps gérées associés à ce profil d’inscription sont également supprimés.
- *Inscription automatisée des appareils :* L’inscription automatisée des appareils permet aux organisations de configurer et de gérer des appareils dès qu’ils sont sortis de leur boîte (il s’agit du *déploiement sans intervention*). Ces appareils sont *supervisés*, et les utilisateurs ont la possibilité d’empêcher la suppression du profil de GAM par l’utilisateur. L’inscription automatisée des appareils est conçue pour les appareils appartenant à l’organisation.

Application de restrictions aux appareils

Les administrateurs peuvent activer ou désactiver des restrictions pour contribuer à empêcher les utilisateurs d’accéder à une app, à un service ou à une fonctionnalité avec les iPhone, iPad, Mac et Apple TV inscrits à une solution de GAM. Les restrictions sont transmises aux appareils par l’entremise d’entités qui appartiennent à un profil de configuration. Certaines restrictions appliquées à un iPhone peuvent être appliquées à une Apple Watch jumelée.

Gestion des réglages des codes et des mots de passe

Par défaut, le code de l’utilisateur peut être défini comme un numéro d’identification personnel (NIP). Sur les appareils iOS et iPadOS dotés de Touch ID ou de Face ID, la longueur minimale du code est de quatre chiffres. Puisque les codes plus complexes ou plus longs sont plus difficiles à deviner et moins vulnérables aux attaques, ils sont recommandés.

Les administrateurs peuvent imposer l’utilisation de codes complexes et d’autres politiques, soit à l’aide de Microsoft Exchange ActiveSync ou d’une solution de gestion des appareils mobiles (GAM), soit en demandant aux utilisateurs d’installer manuellement des profils de configuration. Un mot de passe administrateur est requis pour l’installation d’une entité de politique de code macOS. Certaines politiques en matière de code peuvent imposer des exigences quant à la longueur, à la composition ou à d’autres attributs des codes.

Application du profil de configuration

Les profils de configuration sont le principal moyen par lequel une solution de GAM distribue et gère des politiques et des restrictions sur les appareils gérés. Si les organisations ont besoin de configurer une quantité importante d'appareils ou de distribuer de nombreux certificats ou réglages personnalisés (de messagerie ou réseau) à de nombreux appareils, les profils de configuration constituent un moyen sûr et sécurisé de procéder.

Profils de configuration

Un *profil de configuration* est un fichier XML (dont le nom se termine par .mobileconfig) constitué d'entités qui chargent des réglages et des informations d'autorisation sur les appareils Apple. Les profils de configuration automatisent la configuration des réglages, des comptes, des restrictions et des informations d'identification. Ces fichiers peuvent être créés par une solution de GAM ou par Apple Configurator 2, ou peuvent être créés manuellement. Avant d'envoyer un profil de configuration à un appareil Apple, les organisations doivent inscrire ce dernier à la solution de GAM au moyen d'un profil d'inscription.

Profils d'inscription

Un *profil d'inscription* est un profil de configuration comportant une entité de GAM qui inscrit l'appareil à la solution de GAM indiquée pour cet appareil. Cela permet à la solution de GAM d'envoyer des commandes et des profils de configuration à l'appareil et d'interroger certains aspects de ce dernier. Lors qu'un utilisateur supprime un profil d'inscription, tous les profils de configuration, les réglages et les apps gérées associés à ce profil d'inscription sont également supprimés. Il ne peut y avoir qu'un seul profil d'inscription à la fois sur un appareil.

Réglages du profil de configuration

Un profil de configuration contient un certain nombre de réglages dans des entités spécifiques pouvant être précisées, y compris (sans s'y limiter) :

- politiques de code et de mot de passe;
- restrictions des fonctionnalités de l'appareil (par exemple la désactivation de la caméra);
- réglages réseau et VPN;
- réglages Microsoft Exchange;
- réglages de Mail;
- réglages de compte;
- réglages de service de répertoire LDAP;
- réglages de service de calendrier CalDAV;
- informations d'identification et clés;
- mises à jour logicielles.

Signature et chiffrement des profils

Il est possible de signer les profils de configuration afin de valider leur origine et de les chiffrer pour contribuer à garantir leur intégrité et à protéger leur contenu. Les profils de configuration pour iOS et iPadOS sont chiffrés à l'aide de la syntaxe de message chiffrée (CMS) indiquée dans la norme RFC 5652 et prenant en charge les algorithmes 3DES et AES128.

Installation des profils

Les utilisateurs peuvent installer des profils de configuration directement sur leurs appareils à l'aide d'Apple Configurator 2, en télécharger à l'aide de Safari, s'en faire envoyer en pièce jointe par courriel, en transférer à l'aide d'AirDrop ou de l'app Fichiers sous iOS et iPadOS, ou en recevoir via une connexion sans fil à partir d'une solution de gestion des appareils mobiles (GAM). Lorsqu'un utilisateur configure un appareil dans Apple School Manager ou Apple Business Manager, l'appareil télécharge et installe un profil pour l'inscription à la GAM. Pour obtenir des informations sur la suppression des profils, consultez la section Aperçu de la GAM dans Réglages de la gestion des appareils mobiles pour administrateurs de TI.

Remarque : Sur les appareils supervisés, il est également possible de verrouiller des profils de configuration, ce qui vise à interdire complètement leur suppression ou à n'autoriser cette dernière qu'au moyen d'un code. Comme beaucoup d'organisations possèdent leurs propres appareils iOS et iPadOS, les profils de configuration qui associent un appareil à une solution de GAM peuvent être supprimés, mais cela a pour conséquence de supprimer également toutes les applications, les données et les informations de configuration gérées.

Inscription automatisée des appareils

Les organisations peuvent automatiser l'inscription des appareils iOS, iPadOS, macOS et tvOS à leur solution de gestion des appareils mobiles (GAM) et remettre les appareils aux utilisateurs sans avoir à les manipuler ou à les préparer. Une fois l'inscription à l'un des services effectuée, les administrateurs n'ont qu'à ouvrir une session sur le site Web du service pour associer le programme à leur solution de GAM. Les appareils achetés peuvent ensuite être assignés à des utilisateurs par l'entremise de la solution de GAM. Pendant la configuration de l'appareil, la protection des données sensibles peut être renforcée en mettant en place des mesures de sécurité appropriées. Par exemple :

- Forcer les utilisateurs à s'authentifier pendant la configuration initiale avec Assistant réglages sur l'appareil Apple.
- Proposer une configuration préliminaire à accès limité et exiger une configuration supplémentaire pour que l'appareil puisse accéder aux données sensibles.

Une fois l'appareil associé à un utilisateur, toutes les configurations, restrictions et commandes configurées par la GAM sont automatiquement installées. Toutes les communications entre les appareils et les serveurs d'Apple sont chiffrées en transit par HTTPS (TLS).

Il est possible de simplifier davantage le processus en supprimant certaines étapes d'Assistant réglages pour que les utilisateurs soient rapidement opérationnels. Les administrateurs déterminent également si les utilisateurs peuvent supprimer le profil de GAM de l'appareil, et contribuent à garantir que les restrictions de l'appareil sont en place tout au long du cycle de vie de l'appareil. Sitôt déballé et activé, l'appareil est automatiquement inscrit à la solution de GAM de l'organisation, et tous les livres, apps et réglages de gestion sont installés selon les directives de l'administrateur de la GAM.

Apple School Manager et Apple Business Manager

Apple School Manager et Apple Business Manager sont des services qui permettent aux administrateurs des TI de déployer les appareils Apple achetés par l'organisation directement auprès d'Apple, d'un fournisseur de services ou d'un revendeur agréé Apple participant.

Au moyen d'une solution de GAM, les administrateurs peuvent simplifier le processus de configuration pour les utilisateurs, configurer les réglages, et distribuer des apps et des livres achetés dans Apple School Manager et Apple Business Manager. Apple School Manager s'intègre également aux systèmes d'information scolaire (SIS), soit directement soit par le protocole SFTP. Par ailleurs, Apple School Manager et Apple Business Manager peuvent utiliser le SCIM (System for Cross-domain Identity Management, système de gestion des identités interdomaines) ou l'authentification fédérée avec Microsoft Azure Active Directory (Azure AD) pour permettre aux administrateurs de créer rapidement des comptes.

Les appareils sous iOS 11, tvOS 10.2 et les versions ultérieures peuvent également être ajoutés à Apple School Manager ou à Apple Business Manager après l'achat à l'aide d'Apple Configurator 2.

Apple maintient des certifications conformes aux normes ISO/CEI 27001 et 27018 pour permettre à ses clients de remplir leurs obligations réglementaires et contractuelles. Ces certifications fournissent à ses clients une attestation indépendante des pratiques d'Apple relatives à la sécurité et à la confidentialité des informations pour les systèmes concernés. Pour en savoir plus, consultez l'article de l'assistance Apple Certifications des services Internet Apple.

Remarque : Pour savoir si un programme Apple est offert dans un pays ou une province, consultez l'article de l'assistance Apple Disponibilité des programmes Apple et modes de paiement pour les établissements d'enseignement et les entreprises.

Supervision des appareils

La *supervision* indique généralement que l'appareil appartient à l'organisation, ce qui permet à celle-ci d'assurer un contrôle supplémentaire sur sa configuration et ses restrictions.

Les appareils iPhone et iPad qui fonctionnent sous iOS 5 ou version ultérieure, et les appareils Apple TV qui fonctionnent sous tvOS 10.2 ou version ultérieure peuvent être supervisés :

- en utilisant Apple Configurator 2

  (pendant ce processus, le contenu de l'appareil est effacé, et toutes les données sont perdues);

- en inscrivant l’appareil à une solution de GAM et en choisissant la supervision au cours du processus d’inscription.

Les ordinateurs Mac peuvent être supervisés si :

- ils fonctionnent sous macOS 11 et sont inscrits à la solution de GAM par l’inscription des appareils;
- ils sont mis à niveau vers macOS 11 et l’inscription à la solution de GAM *a été* approuvée par l’utilisateur;
- ils fonctionnent sous macOS 10.14.4 ou version ultérieure et :
  - les numéros de série des appareils figurent dans Apple School Manager ou Apple Business Manager;
  - ils sont inscrits à une solution de GAM par Apple School Manager ou Apple Business Manager.

Les appareils suivants sont automatiquement supervisés lorsqu’ils sont inscrits à Apple School Manager ou Apple Business Manager :

- iPhone et iPod touch sous iOS 13 ou une version ultérieure;
- iPad sous iPadOS 13.1 ou une version ultérieure;
- Apple TV sous tvOS 13 ou une version ultérieure;
- ordinateurs Mac sous macOS 10.14.4 ou une version ultérieure.

Important : Si l’utilisateur connaît le code, il peut supprimer les profils de configuration installés manuellement des iPhone et des iPad non supervisés, même si l’option est réglée à « Jamais ». Les profils de configuration installés manuellement des ordinateurs Mac peuvent être supprimés au moyen de l’outil de ligne de commande `profiles` ou dans Préférences Système si l’utilisateur dispose du nom et du mot de passe d’un administrateur. À partir de macOS 10.15, tout comme sur iOS et iPadOS, les profils installés au moyen de la solution de GAM doivent être supprimés de la même manière. Sinon, ces profils sont supprimés automatiquement au moment de la désinscription de la solution de GAM.

Sécurité du verrouillage d’activation

L’application du verrouillage d’activation par Apple varie selon que l’appareil est un iPhone, un iPad, un Mac avec puce Apple ou un Mac avec processeur Intel et puce T2 Security d’Apple.

Comportement sur iPhone et iPad

Sur iPhone et iPad, le verrouillage d’activation est mis en application par l’entremise du processus d’activation, tout de suite après l’écran de sélection du réseau Wi-Fi d’Assistant réglages d’iOS et d’iPadOS. Lorsque l’appareil indique qu’il est en cours d’activation, il envoie une demande à un serveur Apple pour obtenir un certificat d’activation. Les appareils dont le verrouillage d’activation est activé requièrent la saisie des informations d’identification iCloud de l’utilisateur ayant activé le verrouillage d’activation. Assistant réglages sous iOS ou iPadOS empêchera l’utilisateur de poursuivre la configuration de l’appareil jusqu’à l’obtention d’un certificat valide.

Comportement sur un Mac avec puce Apple

Dans un Mac avec puce Apple, le LLB vérifie qu'un fichier LocalPolicy valide existe pour l'appareil et que les valeurs du nonce LocalPolicy correspondent aux valeurs stockées dans le composant de stockage sécurisé. Le LLB démarre recoveryOS si :

- aucun fichier LocalPolicy n'existe pour la version actuelle de macOS;
- le fichier LocalPolicy n'est pas valide pour cette version de macOS;
- les valeurs de hachage du nonce LocalPolicy ne correspondent pas aux valeurs de hachage stockées dans le composant de stockage sécurisé.

recoveryOS conclut que l'ordinateur Mac n'est pas activé et communique avec le serveur d'activation pour obtenir un certificat d'activation. Si le verrouillage d'activation de l'appareil est activé, recoveryOS exige la saisie des informations d'identification iCloud de l'utilisateur ayant activé le verrouillage d'activation. Après l'obtention d'un certificat d'activation, la clé de ce certificat est utilisée pour obtenir un certificat RemotePolicy. L'ordinateur Mac utilise la clé LocalPolicy et le certificat RemotePolicy pour produire un fichier LocalPolicy valide. Le LLB n'autorisera pas le démarrage de macOS à moins qu'un fichier LocalPolicy valide ne soit présent.

Comportements sur les ordinateurs Mac avec processeur Intel

Dans un Mac avec processeur Intel et puce T2, le programme interne de la puce en question vérifie qu'un certificat d'activation valide est présent avant d'autoriser le démarrage de macOS. Le programme interne UEFI chargé par la puce T2 est chargé d'interroger l'état d'activation de l'appareil auprès de cette même puce et de démarrer recoveryOS au lieu de macOS si aucun certificat d'activation valide n'est présent. recoveryOS conclut alors que le Mac n'est pas activé et communique avec le serveur d'activation pour obtenir un certificat d'activation. Si le verrouillage d'activation de l'appareil est activé, recoveryOS exige la saisie des informations d'identification iCloud de l'utilisateur ayant activé le verrouillage d'activation. Le programme interne UEFI n'autorisera pas le démarrage de macOS à moins qu'un certificat d'activation valide ne soit présent.

Mode Perdu géré et effacement à distance

Le mode Perdu géré est utilisé pour localiser les appareils supervisés en cas de vol. Une fois localisés, ils peuvent être verrouillés et effacés à distance.

Mode Perdu géré

Si un appareil iOS ou iPadOS supervisé équipé d'iOS 9 ou une version ultérieure est perdu ou volé, un administrateur de la solution de gestion des appareils mobiles (GAM) peut activer le mode Perdu (appelé « mode Perdu géré ») à distance sur cet appareil. Lorsque ce mode est activé, l'utilisateur actif est déconnecté et l'appareil ne peut pas être déverrouillé. L'écran affiche alors un message que l'administrateur peut personnaliser, par exemple un numéro de téléphone à composer si l'appareil est retrouvé. L'administrateur peut aussi demander à l'appareil d'envoyer sa position actuelle (même si le service de localisation est désactivé) et, facultativement, d'émettre un son. Si l'administrateur désactive le mode Perdu géré, ce qui constitue le seul moyen de quitter le mode, l'utilisateur en est avisé par un message sur l'écran verrouillé ou une alerte sur l'écran d'accueil.

Effacement à distance

Les appareils iOS, iPadOS et macOS peuvent être effacés à distance par un administrateur ou un utilisateur (l'effacement instantané à distance est disponible uniquement si FileVault est activé sur un Mac). L'effacement instantané à distance est effectué en éliminant de manière sécurisée la clé de support du stockage effaçable, ce qui rend toutes les données illisibles. Pour l'effacement à distance par Microsoft Exchange ActiveSync, l'appareil confirme la commande auprès du serveur Microsoft Exchange avant de procéder.

Lorsqu'une commande d'effacement à distance est activée à partir de la solution de GAM ou d'iCloud, l'iPhone, l'iPad, l'iPod touch ou le Mac renvoie une confirmation à la solution de GAM et procède à l'effacement.

L'effacement à distance est impossible dans les situations suivantes :

- avec l'inscription par l'utilisateur;
- avec Microsoft Exchange ActiveSync si le compte a été installé avec la fonctionnalité d'inscription par l'utilisateur;
- avec Microsoft Exchange ActiveSync si l'appareil est supervisé.

Les utilisateurs peuvent aussi effacer le contenu d'appareils iOS et iPadOS en leur possession à partir de l'app Réglages. Enfin, comme mentionné précédemment, il est possible de régler les appareils iOS et iPadOS afin que l'effacement soit automatiquement déclenché après un certain nombre de tentatives de déverrouillage par code infructueuses.

Sécurité d'iPad partagé sous iPadOS

Aperçu

iPad partagé est un mode multi-utilisateur destiné aux déploiements d'iPad. Il permet aux utilisateurs de partager un iPad tout en maintenant la séparation des documents et des données pour chaque utilisateur. Chaque utilisateur a son propre emplacement de stockage réservé, qui est implanté en tant que volume APFS (système de fichiers d'Apple) protégé par les informations d'identification de l'utilisateur. iPad partagé requiert l'utilisation d'un identifiant Apple géré émis par l'organisation, dont celle-ci demeure propriétaire, et permet à un utilisateur de se connecter sur n'importe quel appareil de l'entreprise configuré pour plusieurs utilisateurs. Les données des utilisateurs sont réparties dans des répertoires distincts, chacun dans son propre domaine de protection des données, et protégées par les autorisations UNIX et le bac à sable. Sous iPadOS 13.4 et les versions ultérieures, les utilisateurs peuvent également ouvrir une session temporaire. Lorsque l'utilisateur met fin à une session temporaire, son volume APFS est supprimé et son espace réservé, retourné au système.

Connexion à iPad partagé

Les identifiants Apple gérés natifs et fédérés sont pris en charge lors de la connexion à iPad partagé. Lors de la première utilisation d'un compte fédéré, l'utilisateur est redirigé vers le portail de connexion du fournisseur d'identité. Après l'authentification, un jeton d'accès éphémère est délivré pour les identifiants Apple gérés, et le processus de connexion se poursuit comme celui des identifiants Apple gérés natifs. Après la connexion, Assistant réglages sur iPad partagé invite l'utilisateur à définir un code (d'identification) pour sécuriser les données locales sur l'appareil et s'identifier sur l'écran de connexion à l'avenir. Comme pour un appareil à un seul utilisateur, sur lequel l'utilisateur se connecte une fois avec son identifiant Apple géré associé à son compte fédéré avant de pouvoir déverrouiller son appareil à l'aide de son code, l'utilisateur d'iPad partagé se connecte une fois à son compte fédéré, puis utilise son code par la suite.

Lorsqu'un utilisateur se connecte sans authentification fédérée, l'identifiant Apple géré est authentifié par le service d'identité d'Apple (IDS, Apple Identity Service) en faisant appel au protocole SRP. Si l'authentification aboutit, un jeton d'accès éphémère, associé à l'appareil, est accordé. Si l'utilisateur s'est déjà servi de l'appareil, il dispose déjà d'un compte utilisateur local qui est alors déverrouillé avec les mêmes informations d'identification.

Si l'utilisateur ne s'en est jamais servi ou s'il utilise la fonctionnalité de session temporaire, iPad partagé fournit un nouvel identifiant d'utilisateur UNIX, un volume APFS pour stocker les données personnelles de l'utilisateur et un trousseau local. Puisque l'espace de stockage est alloué (réservé) à l'utilisateur lors de la création du volume APFS, l'espace pourrait être insuffisant pour créer un nouveau volume. Dans ce cas, le système déterminera un utilisateur dont la synchronisation infonuagique des données est terminée et le supprimera de l'appareil afin de permettre au nouvel utilisateur de se connecter. Dans l'éventualité improbable où le téléchargement dans le nuage des données de tous les utilisateurs n'est pas terminé, la connexion du nouvel utilisateur échoue. Pour se connecter, le nouvel utilisateur devra attendre que la synchronisation des données d'un utilisateur soit terminée ou demander à un administrateur de forcer la suppression d'un compte d'utilisateur existant, risquant ainsi une perte de données.

Si l'appareil n'est pas connecté à Internet (si l'utilisateur n'a pas de point d'accès Wi-Fi, par exemple), l'authentification peut se faire par le compte local pour un nombre de jours limité. Dans ce cas, seuls les utilisateurs qui possèdent déjà un compte local ou qui ouvrent une session temporaire peuvent se connecter. Une fois le délai expiré, les utilisateurs doivent s'authentifier en ligne, même si un compte local existe déjà.

Après le déverrouillage ou la création du compte local de l'utilisateur, si ce dernier s'authentifie à distance, le jeton éphémère délivré par les serveurs d'Apple est converti en jeton iCloud permettant de se connecter à iCloud. Les réglages de l'utilisateur sont ensuite restaurés, et ses documents et données sont synchronisés à partir d'iCloud.

Tant que la session est active et que l'appareil est connecté, ces documents et données sont stockés sur iCloud à mesure que l'utilisateur les crée et modifie. En outre, un mécanisme de synchronisation en arrière-plan contribue à faire en sorte que les modifications sont envoyées à iCloud ou à d'autres services Web à l'aide de sessions NSURLSession en arrière-plan une fois que l'utilisateur se déconnecte. Une fois la synchronisation en arrière-plan terminée pour cet utilisateur, le volume APFS de ce dernier est démonté et ne peut plus être monté sans que l'utilisateur doive se reconnecter.

Les sessions temporaires ne synchronisent pas de données avec iCloud et, bien qu'une session temporaire puisse se connecter à un service de synchronisation tiers comme Box ou Google Drive, aucune fonction ne permet la poursuite de la synchronisation après la fin de la session temporaire.

Déconnexion d'iPad partagé

Lorsqu'un utilisateur se déconnecte d'iPad partagé, son conteneur de clés est immédiatement verrouillé et toutes les apps sont fermées. Pour accélérer la connexion d'un nouvel utilisateur, iPadOS reporte temporairement certaines actions de déconnexion ordinaires et affiche une fenêtre de connexion. Si un nouvel utilisateur se connecte pendant cette période (environ 30 secondes), iPad partagé effectue le nettoyage reporté dans le cadre de la connexion au compte du nouvel utilisateur. Cependant, si iPad partagé demeure inactif, le nettoyage reporté est déclenché. Au cours de la phase de nettoyage, la fenêtre de connexion est redémarrée comme si une autre déconnexion avait eu lieu.

Lorsqu'on met fin à une session temporaire, iPad partagé exécute la séquence de déconnexion complète et supprime immédiatement le volume APFS de la session temporaire.

Sécurité d'Apple Configurator 2

Apple Configurator 2 propose une solution flexible, sécurisée et axée sur l'appareil qui permet à l'administrateur de configurer facilement et rapidement un seul appareil ou plusieurs dizaines d'appareils iOS, iPadOS et tvOS connectés à un Mac par USB (ou d'appareils tvOS jumelés par Bonjour) avant de les remettre aux utilisateurs. Grâce à Apple Configurator 2, l'administrateur peut mettre à jour des logiciels, installer des apps et des profils de configuration, renommer et modifier le fond d'écran des appareils, exporter les données et les documents des appareils, et plus encore.

L'administrateur peut aussi ajouter des appareils iOS, iPadOS et tvOS à Apple School Manager ou Apple Business Manager avec Apple Configurator 2, même si les appareils n'ont pas été achetés directement auprès d'Apple, d'un revendeur agréé Apple ou d'un fournisseur de services mobiles. Quand l'administrateur configure un appareil inscrit manuellement, celui-ci est automatiquement supervisé et inscrit à la solution de gestion des appareils mobiles (GAM), comme tout autre appareil inscrit. Pour les appareils qui n'ont pas été achetés directement auprès d'Apple, d'un revendeur agréé Apple ou d'un fournisseur de services mobiles, les utilisateurs disposent de 30 jours pour retirer leur appareil de l'inscription, de la supervision et de la GAM. Cette période commence après l'activation de l'appareil.

Si les appareils iOS, iPadOS et tvOS n'ont aucun accès à Internet et qu'ils sont connectés à un Mac hôte connecté à Internet pendant leur configuration, les organisations peuvent utiliser Apple Configurator 2 pour les activer. L'administrateur peut restaurer, activer et préparer des appareils en y incluant la configuration nécessaire, y compris des apps, des profils et des documents, et ce, sans avoir à les connecter à un réseau Wi-Fi ou cellulaire. Cette fonctionnalité ne permet pas à un administrateur de contourner toute exigence existante quant au verrouillage d'activation normalement requise au cours d'une activation normale.

Sécurité de Temps d’écran

Sous iOS 12, iPadOS, macOS 10.15, watchOS 6 et les versions ultérieures de ces systèmes d’exploitation, Temps d’écran est une fonctionnalité qui permet aux utilisateurs de connaître et de contrôler leur propre utilisation d’apps et du Web, ainsi que celle de leurs enfants. Bien que Temps d’écran ne soit pas une nouvelle fonctionnalité de sécurité du système, il est important de comprendre comment elle protège la sécurité et la confidentialité des données recueillies et partagées entre les appareils.

Dans Temps d’écran, il existe deux types d’utilisateurs : adultes et enfants.

Le tableau ci-dessous décrit les fonctionnalités principales de Temps d’écran.

Fonctionnalité	Systèmes d’exploitation compatibles
Consulter les données sur l’utilisation	iOS iPadOS macOS
Imposer des restrictions supplémentaires	iOS iPadOS macOS watchOS
Fixer des limites de temps sur le Web	iOS iPadOS macOS
Définir des limites d’app	iOS iPadOS macOS watchOS
Configurer Temps d’arrêt	iOS iPadOS macOS watchOS

Pour les utilisateurs qui gèrent leur propre utilisation de l’appareil, les données sur l’utilisation et les contrôles de Temps d’écran peuvent être synchronisées entre les appareils associés au même compte iCloud l’aide du chiffrement bout en bout CloudKit. Il faut que l’authentification à deux facteurs soit activée sur le compte de l’utilisateur (la synchronisation est activée par défaut). Temps d’écran remplace la fonctionnalité Restrictions des versions antérieures d’iOS et d’iPadOS, ainsi que la fonctionnalité Contrôle parental des versions antérieures de macOS.

Sous iOS 13, iPadOS 13.1, macOS 10.15 et les versions ultérieures de ces systèmes d’exploitation, les utilisateurs de Temps d’écran et les enfants sous leur surveillance partagent automatiquement leur utilisation entre les appareils si l’authentification à deux facteurs est activée pour leur compte iCloud. Lorsqu’un utilisateur vide son historique Safari ou qu’il supprime une app, les données sur l’utilisation correspondantes sont effacées de l’appareil et de tous les appareils synchronisés.

Parents et Temps d’écran

Les parents peuvent aussi utiliser Temps d’écran sur les appareils iOS, iPadOS et macOS pour connaître et contrôler l’utilisation qu’en font leurs enfants. Si le parent est un organisateur (dans le partage familial iCloud), il peut voir les données sur l’utilisation et gérer les réglages de Temps d’écran pour ses enfants. Les enfants sont avisés quand leurs parents activent Temps d’écran, et ils peuvent également suivre leur propre utilisation. Lorsque les parents activent Temps d’écran pour leurs enfants, ils règlent un code pour empêcher leurs enfants d’apporter des modifications. À l’âge de la majorité (l’âge varie selon le pays ou la province), les enfants peuvent désactiver cette surveillance.

Les données sur l’utilisation et les réglages de configuration sont transférés entre l’appareil du parent et ceux des enfants à l’aide du protocole du service d’identité d’Apple (IDS) chiffré de bout en bout. Les données chiffrées peuvent être stockées pour une courte période sur les serveurs de l’IDS jusqu’à ce qu’elles soient lues par l’appareil récepteur (par exemple aussitôt que l’iPhone, l’iPad ou l’iPod touch est mis en marche s’il était éteint). Apple ne peut pas lire ces données.

Analyses de Temps d’écran

Si l’utilisateur active « Partager les analyses », seules les données anonymisées suivantes sont recueillies afin qu’Apple puisse mieux comprendre l’utilisation faite de Temps d’écran :

- si Temps d’écran a été activé avec Assistant réglages ou plus tard dans Réglages;
- si la catégorie d’utilisation a été modifiée après la création d’une limite (dans un délai de 90 jours);
- si Temps d’écran est activé;
- si Temps d’arrêt est activé;
- le nombre de fois que la requête « Demander plus de temps » a été utilisée;
- le nombre de limites d’app;
- le nombre de fois que les utilisateurs ont consulté l’utilisation dans les réglages de Temps d’écran, par type d’utilisateur et par type d’affichage (local, à distance, widget);
- le nombre de fois que les utilisateurs ont ignoré une limite, par type d’utilisateur;
- le nombre de fois que les utilisateurs ont supprimé une limite, par type d’utilisateur.

Apple ne recueille pas de données sur l’utilisation d’apps et de sites Web précis. Lorsqu’un utilisateur voit une liste d’apps dans les informations d’utilisation de Temps d’écran, les icônes d’apps sont extraites directement de l’App Store, ce qui ne conserve aucune donnée de ces demandes.

Glossaire

accès direct à la mémoire (DMA) Une fonctionnalité qui permet aux sous-systèmes de l'appareil d'accéder à la mémoire principale indépendante du processeur central.

AES (norme de chiffrement avancé) Norme de chiffrement mondialement répandue qui sert à chiffrer les données pour les protéger.

AES-XTS Mode AES défini dans la norme IEEE 1619-2007 et destiné au chiffrement des supports de stockage.

algorithme de signature numérique basé sur les courbes elliptiques (ECDSA) ECDSA (Elliptic Curve Digital Signature Algorithm) est un algorithme de signature numérique basé sur la cryptographie sur les courbes elliptiques.

APFS (système de fichiers d'Apple) Le système de fichiers par défaut d'iOS, d'iPadOS, de tvOS, de watchOS et des ordinateurs Mac sous macOS 13.13 ou version ultérieure. L'APFS se caractérise par un chiffrement robuste, le partage d'espace, les instantanés, le calcul rapide des tailles de répertoire et les fondations améliorées du système de fichiers.

Apple Business Manager Apple Business Manager est un portail Web convivial destiné aux administrateurs des TI. Il offre une façon rapide et simplifiée de déployer les appareils Apple que les entreprises ont achetés directement auprès d'Apple, d'un revendeur agréé Apple ou d'un fournisseur de services participant. Les administrateurs peuvent automatiser l'inscription des appareils à leur solution de gestion des appareils mobiles (GAM) et remettre les appareils aux utilisateurs sans avoir à les manipuler ou à les préparer.

Apple School Manager Apple School Manager est un portail Web convivial destiné aux administrateurs des TI. Il offre une façon rapide et simplifiée de déployer les appareils Apple que les établissements d'enseignement ont achetés directement auprès d'Apple, d'un revendeur agréé Apple ou d'un fournisseur de services participant. Les administrateurs peuvent automatiser l'inscription des appareils à leur solution de gestion des appareils mobiles (GAM) et remettre les appareils aux utilisateurs sans avoir à les manipuler ou à les préparer.

autorisation du logiciel système Processus qui combine des clés de chiffrement intégrées au matériel avec un service en ligne pour vérifier que seuls les logiciels légitimes d'Apple, qui conviennent aux appareils pris en charge, sont fournis et installés au moment de la mise à niveau.

bits de départ de logiciel Bits dédiés dans le moteur AES du Secure Enclave qui sont ajoutés à l'UID lors de la génération de clés à partir de l'UID. Chaque bit de départ de logiciel détient un bit de verrouillage correspondant. La mémoire morte d'amorçage et le système d'exploitation du Secure Enclave peuvent modifier, de façon indépendante, la valeur de chacun des bits de départ de logiciel pourvu que le bit de verrouillage correspondant n'ait pas été réglé. Une fois qu'il est réglé, le bit de verrouillage, ainsi que le bit de départ de logiciel, ne peut plus être modifié. Les bits de départ de logiciel et leur bit de verrouillage sont réinitialisés au redémarrage du Secure Enclave.

Boot Camp Utilitaire qui prend en charge l'installation de Microsoft Windows sur les ordinateurs Mac compatibles.

cartographie angulaire de la direction des crêtes Représentation mathématique de la direction et de la largeur des crêtes extraites d'une partie d'empreinte digitale.

chargeur d'amorçage de niveau inférieur (LLB) Sur les ordinateurs Mac dotés d'une architecture de démarrage à deux étapes, le LLB contient le code appelé par la mémoire morte d'amorçage, qui charge à son tour iBoot dans le cadre d'une chaîne de démarrage sécurisé.

circuit intégré (CI) Également appelé *micropuce*.

CKRecord Dictionnaire des paires clé-valeur qui contiennent des données enregistrées ou récupérées dans CloudKit.

clé de support Partie de la hiérarchie des clés de chiffrement qui permet d'offrir un effacement sécurisé et instantané. Sous iOS, iPadOS, tvOS et watchOS, la clé de support enveloppe les métadonnées sur le volume de données (sans elle, l'accès à toutes les clés par fichier est impossible, ce qui rend inaccessibles les fichiers protégés par la protection des données). Sous macOS, la clé de support enveloppe le matériel de chiffrement, les métadonnées et les données sur le volume protégé par FileVault. Dans les deux cas, l'effacement de la clé de support rend les données chiffrées inaccessibles.

clé dérivée du code (PDK) La clé de chiffrement dérivée de l'emmêlement du mot de passe de l'utilisateur avec la clé SKP à long terme et l'UID du Secure Enclave.

clé du système de fichiers Clé permettant de chiffrer les métadonnées de chaque fichier, y compris la clé de classe. Elle est conservée dans le stockage effaçable pour permettre l'effacement rapide plutôt que pour des raisons de confidentialité.

clé par fichier Clé utilisée par la protection des données pour chiffrer un fichier sur le système de fichiers. La clé par fichier est enveloppée par une clé de classe et stockée dans les métadonnées du fichier.

composant de stockage sécurisé Une puce dotée d'un code immuable en lecture seule, d'un générateur de nombres aléatoires matériel, de moteurs de chiffrement et d'un détecteur de sabotage physique. Sur les appareils compatibles, le Secure Enclave est jumelé à un composant de stockage sécurisé pour le stockage des nonces antirejeu. Pour lire et mettre à jour les nonces, le Secure Enclave et la puce de stockage ont recours à un protocole sécurisé qui contribue à garantir un accès exclusif aux nonces. Il existe plusieurs générations de cette technologie dont les garanties en matière de sécurité diffèrent.

conteneur de clés Structure de données utilisée pour stocker une collection de clés de classe. Chaque type (utilisateur, appareil, système, sauvegarde, autorité de séquestre ou sauvegarde iCloud) possède le même format.

Un en-tête contenant : la version (réglée à quatre sous iOS 12 ou les versions ultérieures), le type (système, sauvegarde, autorité de séquestre ou sauvegarde iCloud), l'UUID du conteneur de clés, un code HMAC si le conteneur de clés est signé, la méthode utilisée pour envelopper les clés de classe (emmêler les clés avec l'UID ou PBKDF2), ainsi que le sel et le nombre d'itérations.

Une liste de clés de classe : UUID de clé, classe (classe de protection des données du trousseau ou de fichiers), type d'enveloppement (clé dérivée de l'UID uniquement; clé dérivée de l'UID et clé dérivée du code), clé de classe enveloppée et clé publique pour classes asymétriques.

contrôleur de mémoire Sous-système du système sur une puce qui contrôle l'interface entre celui-ci et sa mémoire principale.

contrôleur SSD Sous-système matériel qui gère le support de stockage (disque SSD).

Data Vault Mécanisme imposé par le noyau qui vise à protéger les données contre tout accès non autorisé, que l'app demandeuse soit mise en bac à sable ou non.

distribution aléatoire de l'espace d'adressage (ASLR) Technique utilisée par les systèmes d'exploitation pour rendre plus difficile l'exploitation d'un bogue de logiciel. Comme les décalages et les adresses mémoire sont imprévisibles, le code d'exploit ne peut pas coder ces valeurs en dur.

Échange Diffie-Hellman à courbe elliptique (ECDHE) Échange Diffie-Hellman à courbe elliptique faisant appel à des clés éphémères. L'ECDHE permet à deux parties de s'entendre sur une clé secrète d'une manière qui empêche la clé d'être découverte par l'interception illicite des messages entre les deux parties.

emmêlement Processus par lequel le code d'un utilisateur est transformé en clé de chiffrement et renforcé à l'aide de l'UID de l'appareil. Ce processus contribue à garantir que les attaques en force ne peuvent être exécutées que sur un appareil donné à la fois, ce qui empêche les attaques massives menées en parallèle. L'algorithme d'emmêlement est le PBKDF2, qui utilise une clé AES avec l'UID de l'appareil comme fonction pseudo-aléatoire pour chaque itération.

enveloppement de clé Chiffrement d'une clé à l'aide d'une autre clé. iOS et iPadOS utilisent l'algorithme NIST AES conformément à la norme RFC 3394.

eSPI Bus d'interface périphérique série améliorée destiné à la communication en série synchrone.

gestion des appareils mobiles (GAM) Service qui permet à un administrateur de gérer à distance les appareils inscrits. Une fois qu'un appareil est inscrit, l'administrateur peut utiliser le service de GAM sur le réseau pour configurer les réglages et effectuer d'autres tâches sur l'appareil sans devoir interagir avec son utilisateur.

HMAC Il s'agit d'un code d'authentification de message basé sur une fonction de hachage cryptographique.

iBoot Code qui charge XNU, dans le cadre d'une chaîne de démarrage sécurisé. Selon la génération du système sur une puce, iBoot peut être chargé soit par le chargeur d'amorçage de niveau inférieur (LLB), soit directement par la mémoire morte d'amorçage.

identifiant de groupe (GID) Semblable à l'UID, mais commun à tous les processeurs d'une classe.

identifiant de ressource uniforme (URI) Chaîne de caractères permettant d'identifier une ressource Web.

identifiant unique (UID) Clé AES 256 bits gravée sur chaque processeur au moment de sa fabrication. Elle ne peut être lue ni par le programme interne ni par le logiciel, et elle n'est utilisée que par le moteur AES matériel du processeur. Pour trouver cette clé, un assaillant devrait lancer une attaque physique onéreuse et extrêmement sophistiquée contre la puce du processeur. L'UID n'est lié à aucun autre identifiant présent sur l'appareil, comme l'UDID.

identifiant unique de puce (ECID) Identifiant 64 bits propre au processeur de chaque appareil iOS et iPadOS. Si un appel est pris sur un appareil, la sonnerie sur les appareils à proximité et jumelés via iCloud est coupée par une brève notification Bluetooth faible énergie (BLE) 4.0. Les octets de cette notification sont chiffrés par la même méthode que les notifications de type Handoff. Cet identifiant est utilisé dans le cadre du processus de personnalisation et n'est pas considéré comme un secret.

JTAG (Joint Test Action Group) Outil de débogage matériel standard utilisé par les programmeurs et les développeurs de circuits.

mémoire morte d'amorçage Tout premier code exécuté par le processeur d'un appareil lors du démarrage de ce dernier. Comme ce code fait partie intégrante du processeur, il ne peut être modifié ni par Apple ni par un assaillant.

mode de mise à niveau du programme interne de l'appareil (DFU) Mode d'attente adopté par le code de la mémoire morte d'amorçage d'un appareil avant une récupération au moyen d'une connexion USB. L'écran est noir en mode DFU, mais l'invite ci-dessous est affichée dès la connexion à un ordinateur exécutant iTunes ou le Finder : « iTunes [ou le Finder] a détecté un [iPad, iPhone ou iPod touch] en mode de récupération. L'utilisateur doit restaurer cet [iPad, iPhone ou iPod touch] avant de pouvoir l'utiliser avec iTunes [ou le Finder]. »

mode de récupération Mode utilisé pour restaurer de nombreux appareils Apple si l'appareil n'est pas reconnu, et ce, afin de permettre à l'utilisateur de réinstaller le système d'exploitation.

module de sécurité matériel (HSM) Ordinateur spécialisé, protégé contre toute manipulation, utilisé pour sauvegarder et gérer des clés numériques.

moteur de chiffrement AES Composant matériel dédié qui met en œuvre la norme AES.

NAND Mémoire flash non volatile.

prime de sécurité d'Apple Récompense remise par Apple aux chercheurs qui signalent une faille portant atteinte à la dernière version des systèmes d'exploitation et, selon le cas, aux appareils les plus récents.

profil d'approvisionnement Une liste de propriétés (fichier .plist) signée par Apple, qui contient un ensemble d'entités et de déclarations d'autorisation qui autorisent des apps à être installées et testées sur un appareil iOS ou iPadOS. Le profil d'approvisionnement de développement répertorie les appareils sélectionnés par un développeur en vue d'une distribution ad hoc. Le profil d'approvisionnement de distribution contient l'identifiant d'une app développée par une entreprise.

programme interne UEFI Le standard UEFI (Unified Extensible Firmware Interface, interface micrologicielle extensible unifiée) est une technologie qui succède au BIOS pour connecter le programme interne au système d'exploitation d'un ordinateur.

protection de l’intégrité du coprocesseur système (SCIP) Mécanisme utilisé par Apple qui contribue à prévenir les modifications du programme interne du coprocesseur.

protection des données Mécanisme de protection des fichiers et des trousseaux pour les appareils Apple compatibles. Cette expression peut également faire référence aux API utilisées par des apps pour protéger des fichiers et des éléments du trousseau.

protection scellée des clés (SKP) Technologie de la protection des données qui protège, ou *scelle*, les clés de chiffrement à l’aide de mesures de logiciels et de clés système disponibles uniquement au niveau matériel (comme l’UID du Secure Enclave).

registre de progression du démarrage (BPR) Ensemble d’indicateurs matériels des systèmes sur une puce qu’un logiciel peut utiliser pour surveiller les différents modes de démarrage que l’appareil a déclenchés, comme le mode DFU (mise à niveau du programme interne de l’appareil) ou le mode de récupération. Une fois activé, un indicateur BPR ne peut plus être désactivé. Cela permet à un logiciel de disposer par la suite d’un indicateur fiable de l’état du système.

sepOS Programme interne du Secure Enclave, qui repose sur une version personnalisée par Apple du micronoyau L4.

service d’identité d’Apple (IDS) Répertoire Apple contenant les clés publiques d’iMessage, les adresses de service APN, les numéros de téléphone et les adresses électroniques utilisés pour la recherche d’adresses d’appareil et de clés.

service de notifications Push d’Apple (APN) Service mondial offert par Apple pour fournir des notifications de type Push aux appareils Apple.

stockage effaçable Zone dédiée de l’espace de stockage NAND, utilisée pour stocker des clés de chiffrement. Il est possible de l’adresser directement et de l’effacer de manière sécurisée. Bien qu’elle n’offre aucune protection si un assaillant a l’appareil en sa possession, les clés conservées dans le stockage effaçable peuvent être utilisées dans le cadre d’une hiérarchie de clés pour faciliter l’effacement rapide et renforcer la sécurité.

système sur une puce Circuit intégré (CI) réunissant plusieurs composants sur une seule puce. Le processeur d’application, le Secure Enclave et les autres coprocesseurs sont des composants du système sur une puce.

trousseau L’infrastructure et un ensemble d’API utilisés par les systèmes d’exploitation Apple et les apps tierces pour stocker et récupérer des mots de passe, des clés et d’autres informations d’identification délicates.

unité de gestion de la mémoire d’entrée/sortie (UGMES) Sous-système d’une puce intégrée qui contrôle l’accès à l’espace d’adressage à partir des autres appareils et périphériques d’entrée/sortie.

xART Abréviation de « eXtended Anti-Replay Technology » (technologie antirejeu étendue), un ensemble de services qui fournit du stockage persistant chiffré et authentifié pour le Secure Enclave et qui comporte des fonctionnalités antirejeu reposant sur l’architecture de stockage matérielle. Voir la rubrique « composant de stockage sécurisé ».

XNU Noyau au centre des systèmes d’exploitation Apple. Il est supposé fiable et permet d’appliquer des mesures de sécurité telles que la signature de code, la mise en bac à sable, la vérification des déclarations d’autorisation et la distribution aléatoire de l’espace d’adressage (ASLR).

Historique des révisions du document

Date	Résumé
Mai 2021	Actualisé pour : • iOS 14.5 • iPadOS 14.5 • macOS 11.3 • tvOS 14.5 • watchOS 7.4 Sujets ajoutés : • Clavier Magic Keyboard doté de Touch ID • Intention sécurisée et connexions au Secure Enclave • Déverrouillage automatique et Apple Watch • Hachage du manifeste Image4 de CustomOS (coih) Sujets modifiés : • Ajout de deux nouvelles transactions du mode Express dans la section Mode Express pour les cartes accessibles en mode Réserve • Modification de la section Résumé des fonctionnalités du Secure Enclave • Contenu lié à la mise à jour logicielle ajouté à la section Multidémarrage sécurisé (smb3) • Contenu ajouté à la section Protection scellée des clés (SKP)

Date	Résumé
Février 2021	Actualisé pour : • iOS 14.3 • iPadOS 14.3 • macOS 11.1 • tvOS 14.3 • watchOS 7.2 Sujets ajoutés : • Implémentation iBoot à mémoire sécurisée • Processus de démarrage d'un Mac avec puce Apple • Modes de démarrage d'un Mac avec puce Apple • Contrôle du règlement de sécurité du disque de démarrage d'un Mac avec puce Apple • Création et gestion de la clé de signature du fichier LocalPolicy • Contenu d'un fichier LocalPolicy d'un Mac avec puce Apple • Sécurité du volume système signé sous macOS • Appareil de recherche en sécurité d'Apple • Surveillance des mots de passe • Sécurité IPv6 • Sécurité des clés de véhicule sous iOS Sujets mis à jour : • Secure Enclave • Déconnexion matérielle du micro • Environnements de diagnostic et recoveryOS d'un Mac avec processeur Intel • Protections de l'accès direct à la mémoire des ordinateurs Mac • Extensions de noyau sous macOS • Protection de l'intégrité du système • Sécurité du système sous watchOS • Gestion de FileVault sous macOS • Accès des apps aux mots de passe enregistrés • Avis relatifs à la sécurité des mots de passe • Sécurité d'Apple Cash sous iOS, iPadOS et watchOS • Clavardage commercial sécurisé avec l'app Messages • Confidentialité Wi-Fi • Sécurité du verrouillage d'activation • Sécurité d'Apple Configurator 2

Date	Résumé
Avril 2020	Actualisé pour : • iOS 13.4 • iPadOS 13.4 • macOS 10.15.4 • tvOS 13.4 • watchOS 6.2 Mises à jour : • Ajout de la déconnexion du microphone de l'iPad à la section Déconnexion matérielle du micro • Ajout de Data Vault à la section Protections contre l'accès des apps aux données utilisateur • Mises à jour apportées aux sections Gestion de File Vault sous macOS et Outils de ligne de commande • Ajouts de l'outil de suppression de logiciels malveillants dans la section Protection contre les logiciels malveillants sous macOS • Mises à jour apportées à la section Sécurité d'iPad partagé sous iPadOS
Décembre 2019	Fusion du guide sur la sécurité iOS, de l'aperçu de la sécurité sous macOS et de l'aperçu de la puce T2 Security d'Apple Actualisé pour : • iOS 13.3 • iPadOS 13.3 • macOS 10.15.2 • tvOS 13.3 • watchOS 6.1.1 Les sections Contrôles de confidentialité, Siri, Suggestions Siri et Prévention intelligente du suivi dans Safari ont été supprimées. Consultez https://www.apple.com/ca/fr/privacy/ pour obtenir l'information la plus récente sur ces fonctionnalités.
Mai 2019	Actualisé pour iOS 12.3 • Prise en charge de TLS 1.3 • Description de la sécurité AirDrop révisée • Mode DFU et mode de récupération • Exigences relatives au code pour les connexions d'accessoires
Novembre 2018	Actualisé pour iOS 12.1 • FaceTime en groupe

Date	Résumé
Septembre 2018	Actualisé pour iOS 12 • Secure Enclave • Protection de l’intégrité du système d’exploitation • Mode Express pour les cartes accessible en mode Réserve • Mode DFU et mode de récupération • Accessoires de télécommande HomeKit • Cartes sans contact • Cartes étudiantes • Suggestions de Siri • Raccourcis dans Siri • App Raccourcis • Gestion des mots de passe d’utilisateur • Temps d’écran • Certificats et programmes de sécurité
Juillet 2018	Actualisé pour iOS 11.4 • Politiques relatives à la biométrie • HomeKit • Apple Pay • Clavardage commercial • Messages dans iCloud • Apple Business Manager
Décembre 2017	Actualisé pour iOS 11.2 • Apple Pay Cash
Octobre 2017	Actualisé pour iOS 11.1 • Certificats et programmes de sécurité • Touch ID et Face ID • Notes partagées • Chiffrement de bout en bout CloudKit • Mise à jour sur le protocole TLS • Apple Pay, utilisation d’Apple Pay en ligne • Suggestions de Siri • iPad partagé
Juillet 2017	Actualisé pour iOS 10.3 • Secure Enclave • Protection des données des fichiers • Conteneurs de clés • Certificats et programmes de sécurité • SiriKit • HealthKit • Sécurité des réseaux • Bluetooth • iPad partagé • Mode Perdu • Verrouillage d’activation • Contrôles de confidentialité

Date	Résumé
Mars 2017	Actualisé pour iOS 10 • Sécurité du système • Classes de protection des données • Certificats et programmes de sécurité • HomeKit, ReplayKit, SiriKit • Apple Watch • Wi-Fi, VPN • Authentification unique • Apple Pay, utilisation d'Apple Pay en ligne • Transfert des cartes de crédit, de débit et prépayées • Suggestions Safari
Mai 2016	Actualisé pour iOS 9.3 • Identifiant Apple géré • Authentification à deux facteurs pour l'identifiant Apple • Conteneurs de clés • Certifications de sécurité • Mode Perdu, verrouillage d'activation • Notes sécurisées • Apple School Manager • iPad partagé
Septembre 2015	Actualisé pour iOS 9 • Verrouillage d'activation de l'Apple Watch • Politiques en matière de code • Prise en charge de l'API Touch ID • Protection des données sur l'A8 avec AES-XTS • Conteneurs de clés pour la mise à jour logicielle sans surveillance • Mises à jour de certification • Modèle de confiance des apps d'entreprise • Protection des données pour les signets Safari • Fonctionnalité App Transport Security • Spécifications VPN • Accès à distance iCloud pour HomeKit • Cartes de fidélité Apple Pay, app de l'émetteur de cartes Apple Pay • Indexation Spotlight sur l'appareil • Modèle de jumelage iOS • Apple Configurator 2 • Restrictions

Apple Inc.

Apple
One Apple Park Way
Cupertino, CA 95014
USA
apple.com

C028-00309