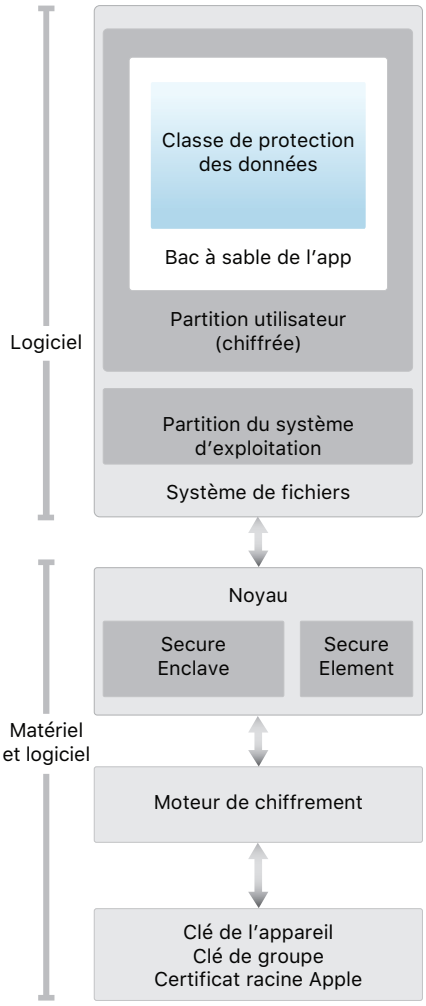
Sécurité iOS

iOS 12.3

Mai 2019

Table des matières

Introduction



Le schéma de l'architecture de sécurité d'iOS fournit une vue d'ensemble des différentes technologies présentées dans ce document.

Apple a conçu la plateforme iOS en mettant l'accent sur la sécurité. Quand nous avons entrepris de créer la meilleure plateforme mobile qui soit, nous avons mis à profit plusieurs décennies d'expérience pour mettre au point une architecture entièrement nouvelle. Nous avons pris en compte les risques de sécurité de l'environnement de bureau et adopté une nouvelle approche de la sécurité lors de la conception d'iOS. Nous avons développé et intégré des fonctionnalités innovantes qui renforcent la sécurité mobile et protègent l'ensemble du système par défaut. iOS constitue donc une avancée majeure en matière de sécurité des appareils mobiles.

Chaque appareil iOS combine des technologies logicielles et matérielles, et des services qui fonctionnent ensemble pour offrir une sécurité et une transparence maximales sans interférer avec l'expérience de l'utilisateur. iOS protège non seulement l'appareil et ses données, mais également l'ensemble de l'écosystème, notamment tout ce que les utilisateurs font localement, sur les réseaux et avec des services internet clés.

Même si iOS et les appareils iOS offrent des fonctionnalités de sécurité avancées, ils n'en restent pas moins simples d'utilisation. Bon nombre de ces fonctionnalités étant activées par défaut, les services informatiques n'ont pas à réaliser de configurations importantes. En outre, les fonctionnalités de sécurité clés comme le chiffrement de l'appareil ne sont pas configurables et ne peuvent donc pas être désactivées par mégarde. D'autres fonctionnalités, comme Face ID, améliorent l'expérience de l'utilisateur en lui permettant de sécuriser l'appareil plus simplement et intuitivement.

Le présent document fournit des informations détaillées sur la mise en œuvre des technologies et des fonctionnalités de sécurité au sein de la plateforme iOS. Il aide également les organisations à combiner

les technologies et les fonctionnalités de sécurité de la plateforme iOS avec leurs propres stratégies et procédures pour répondre à leurs besoins spécifiques en matière de sécurité.

Ce document s'articule autour des thèmes suivants :

- **Sécurité du système :** les technologies logicielles et matérielles intégrées et sécurisées qui constituent la plateforme de l'iPhone, de l'iPad et de l'iPod touch.
- **Chiffrement et protection des données :** l'architecture et la conception qui protègent les données 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 non autorisée.
- **Sécurité des apps :** les systèmes qui permettent aux apps de s'exécuter en toute sécurité et sans compromettre l'intégrité de la plateforme.
- **Sécurité du réseau :** les protocoles de mise en réseau standard qui assurent la sécurisation de l'authentification et le chiffrement des données lors des transmissions.
- **Apple Pay :** la technologie des paiements sécurisés d'Apple.
- **Services internet :** l'infrastructure du réseau d'Apple pour la messagerie, la synchronisation et la sauvegarde.

- **Gestion des mots de passe d'utilisateur :** restrictions des mots de passe et accès à ceux-ci par d'autres sources autorisées.
- **Contrôles de l'appareil :** méthodes permettant de gérer des appareils iOS, d'empêcher l'usage non autorisé et d'activer l'effacement à distance si un appareil est perdu ou volé.
- **Contrôles de confidentialité :** les fonctionnalités d'iOS qui permettent de contrôler l'accès au service de localisation et aux données utilisateur.
- **Certificats et programmes de sécurité :** informations sur les certifications ISO, la validation cryptographique, la certification des critères communs et les solutions commerciales pour composants classifiés (CSfC).

Sécurité du système

La sécurité du système est conçue de sorte que tous les composants clés de chaque appareil iOS soient sécurisés, qu'ils soient logiciels ou matériels. Cela inclut le processus de démarrage, les mises à jour du logiciel et le Secure Enclave. Cette architecture est au cœur de la sécurité d'iOS et n'interfère jamais avec la convivialité de l'appareil.

L'intégration étroite des technologies logicielles et matérielles et des services sur les appareils iOS garantit la sécurisation de chaque composant du système et valide celui-ci dans son ensemble. Du démarrage aux apps tierces, en passant par les mises à jour du logiciel iOS, chaque étape est analysée et contrôlée pour s'assurer que le logiciel et le matériel interagissent de manière optimale et utilisent correctement les ressources.

Chaîne de démarrage sécurisée

Chaque étape du processus de démarrage contient des composants qui sont signés de manière cryptographique par Apple pour garantir leur intégrité et qui ne s'exécutent qu'une fois la chaîne de confiance vérifiée. Ces composants regroupent entre autres les chargeurs d'amorçage, le noyau, les extensions du noyau et le programme interne de bande de base. Cette chaîne de démarrage sécurisée permet de s'assurer que les niveaux les plus bas des logiciels ne sont pas altérés.

Lorsqu'un appareil iOS est mis sous tension, son processeur d'application exécute immédiatement un code stocké dans une mémoire en lecture seule appelée **mémoire morte d'amorçage**. Ce code immuable, appelé racine de confiance matérielle, est défini lors de la fabrication de la puce et implicitement considéré comme fiable. Le code de la mémoire morte d'amorçage contient la clé publique d'AC Apple Root, qui est utilisée pour vérifier que le chargeur d'amorçage **iBoot** est signé par Apple avant d'autoriser son chargement. Il s'agit de la première étape de la chaîne de confiance, dans laquelle chaque étape vérifie que la suivante est signée par Apple. Lorsqu'iBoot termine ses tâches, il vérifie et exécute le noyau iOS. Pour les appareils dotés d'un processeur A9 ou d'une version antérieure de la série A, une étape de **chargeur d'amorçage de niveau inférieur (LLB)** supplémentaire est chargée et vérifiée par la mémoire morte d'amorçage et, par conséquent, 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 DFU
- **LLB ou iBoot :** Mode de récupération

Dans les deux cas, l'appareil doit être connecté à iTunes par USB pour rétablir ses réglages par défaut d'origine.

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 il est mis à jour avant le démarrage des modes suivants :

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

Pour en savoir plus, consultez la section « Chiffrement et protection des données » du présent document.

Sur les appareils avec connectivité cellulaire, le sous-système de bande de base fait également appel à un processus de démarrage sécurisé similaire, avec logiciel et clés signés vérifiés par le processeur de bande de base.

Le coprocesseur Secure Enclave emploie aussi un processus de démarrage sécurisé qui garantit que son logiciel indépendant est vérifié et signé par Apple. Consultez la section « Secure Enclave » du présent document.

Pour en savoir plus sur le passage manuel en mode de récupération, rendez-vous sur : https://support.apple.com/HT201263

Autorisation du logiciel système

Apple publie régulièrement des mises à jour logicielles pour traiter les nouveaux problèmes de sécurité et offrir de nouvelles fonctionnalités; ces mises à jour sont disponibles en même temps pour tous les appareils pris en charge. Les utilisateurs reçoivent des notifications de mise à jour d'iOS sur leur appareil et dans iTunes, et les mises à jour sont transmises par le biais d'une connexion sans fil, ce qui favorise l'adoption rapide des derniers correctifs de sécurité.

Le processus de démarrage décrit ci-dessus permet de s'assurer que seul le code signé par Apple peut être installé sur un appareil. Pour empêcher le retour des appareils à une version antérieure ne disposant pas des dernières mises à jour de sécurité, iOS utilise un processus appelé Autorisation du logiciel système. Si le retour à une version antérieure était possible, une personne malintentionnée entrant en possession d'un appareil pourrait installer une ancienne version d'iOS et exploiter une vulnérabilité corrigée dans la version plus récente.

Sur un appareil doté du coprocesseur Secure Enclave, ce dernier fait également appel à l'autorisation du logiciel système pour garantir l'intégrité de son logiciel et empêcher l'installation d'une version antérieure. Consultez la section « Secure Enclave » du présent document.

Les mises à jour du logiciel iOS peuvent être installées sur l'appareil à l'aide d'iTunes ou par le biais d'une connexion sans fil. Avec iTunes, une copie complète d'iOS est téléchargée et installée. Les mises à jour du logiciel effectuées par l'entremise d'une connexion sans fil ne téléchargent que les composants nécessaires à la mise à jour, ce qui améliore l'efficacité du réseau, au lieu de télécharger l'intégralité du système d'exploitation. En outre, les mises à jour du logiciel peuvent être mises en cache sur un Mac sous macOS High Sierra avec la mise en cache de contenu activée, ce qui évite aux appareils iOS de télécharger à nouveau la mise à jour nécessaire sur internet. Une communication avec les serveurs d'Apple est malgré tout nécessaire pour conclure le processus de mise à jour.

Lors d'une mise à niveau d'iOS, iTunes (ou l'appareil lui-même, dans le cas d'une mise à jour sans fil du logiciel) se connecte au serveur d'autorisation d'installation d'Apple et lui envoie une liste de mesures de chiffrement pour chaque partie du lot à installer (par exemple, iBoot, le noyau et l'image du système d'exploitation), une valeur antirépétition aléatoire (nonce) et l'**identifiant de puce exclusif (ECID)** propre à l'appareil.

Le serveur d'autorisation compare alors la liste de mesures qui lui est fournie aux versions pour lesquelles 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 n'accordant son autorisation et sa signature que pour des mesures connues, le serveur garantit que la mise à jour se déroule exactement comme prévu par Apple.

L'évaluation de la chaîne de confiance au démarrage vérifie que la signature provient d'Apple et que la mesure de l'élément chargé à partir du disque, combinée à l'ECID de l'appareil, correspond à ce qui était couvert par la signature. Ces étapes assurent que l'autorisation concerne un appareil en particulier et qu'une ancienne version d'iOS d'un appareil ne peut pas être copiée vers un autre. Le nonce empêche une personne malintentionnée d'enregistrer la réponse du serveur et de l'utiliser pour altérer un appareil ou modifier de quelconque façon le logiciel système.

Secure Enclave

Le Secure Enclave est un coprocesseur intégré à la puce-système. Il utilise une mémoire chiffrée et intègre un générateur de nombres aléatoires matériel. Le Secure Enclave fournit toutes les opérations de chiffrement pour la gestion des clés de **protection des données** et maintient l'intégrité de la protection des données même si le noyau est compromis. La communication entre le Secure Enclave et le processeur d'application est isolée avec une boîte aux lettres à interruptions et des tampons de données à mémoire partagée.

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 racine de confiance matérielle du Secure Enclave.

Le Secure Enclave exécute un système d'exploitation basé sur une version adaptée par Apple de la gamme de micronoyaux L4. Ce système d'exploitation du Secure Enclave est signé par Apple, vérifié par la mémoire morte d'amorçage du Secure Enclave et mis à jour par un processus de mise à jour logicielle personnalisé.

Au démarrage de l'appareil, une clé de protection de mémoire éphémère est créée par la mémoire morte d'amorçage du Secure Enclave, combinée à l'UID de l'appareil, et utilisée pour chiffrer la partie de l'espace mémoire de l'appareil réservée au Secure Enclave. À l'exception de la puce-système A7 d'Apple, la mémoire du Secure Enclave est également authentifiée avec la clé de protection de mémoire. Sur les puces-systèmes A11 (ou plus récente) et S4, un arbre d'intégrité est utilisé pour empêcher la répétition de la mémoire hautement sécurisée du Secure Enclave, qui est authentifiée par la clé de protection de mémoire et les nonces stockés dans la mémoire vive statique (SRAM) de la puce.

Les données enregistrées par le Secure Enclave sur le système de fichiers sont chiffrées à l'aide d'une clé combinée à l'UID et d'un compteur antirépétition. Le compteur antirépétition est stocké dans un **circuit intégré (CI)** à mémoire non volatile dédiée.

Sur les appareils dotés des puces-systèmes A12 et S4, le Secure Enclave est jumelé à un circuit intégré à mémoire stable pour le stockage du compteur antirépétition. Le CI à mémoire stable est doté d'un code immuable en mémoire morte, d'un générateur matériel de nombres aléatoires, de moteurs de chiffrement et d'un détecteur de sabotage physique. Pour lire et mettre à jour les compteurs, le Secure Enclave et le CI de stockage ont recours à un protocole sécurisé qui assure l'accès exclusif aux compteurs.

Les services antirépétition du Secure Enclave sont utilisés pour révoquer des données lorsque des événements franchissent les limites d'antirépétition, y compris, sans s'y limiter, lors des événements suivants :

- modification du code;
- activation ou désactivation de Touch ID ou de Face ID;
- ajout ou suppression d'une empreinte digitale pour Touch ID;
- réinitialisation de Face ID;
- ajout ou suppression d'une carte Apple Pay;
- effacement du contenu ou des réglages.

Le Secure Enclave est également chargé de traiter les données d'empreintes digitales et les données faciales transmises par les capteurs Touch ID et Face ID, de déterminer s'il y a une correspondance, puis d'autoriser l'accès ou un achat au nom de l'utilisateur.

Protection de l'intégrité du système d'exploitation

Protection de l'intégrité du noyau

Une fois l'initialisation du noyau iOS terminée, la protection de l'intégrité du noyau (KIP) est activée pour empêcher les modifications du code du pilote et du noyau. 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. En outre, l'unité de gestion de la mémoire (UGM) du processeur d'application est configurée de manière 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 de la zone de mémoire du noyau.

Le matériel utilisé pour activer la KIP est verrouillé après le processus de démarrage afin d'empêcher la reconfiguration. La KIP est prise en charge par les puces-systèmes A10, S4 ou plus récente.

Protection de l'intégrité du coprocesseur système

Les coprocesseurs système sont des processeurs situés sur la même puce-système que le processeur d'application. Les coprocesseurs système sont réservés à une utilisation précise et le noyau iOS leur délègue plusieurs tâches. Voici quelques exemples :

- Secure Enclave;
- le processeur de capteur d'image;
- le coprocesseur de mouvement.

Puisque le programme interne du coprocesseur gère de nombreuses tâches système essentielles, sa sécurité est un élément important de la sécurité de l'ensemble du système.

La protection de l'intégrité du coprocesseur système (SCIP) utilise un mécanisme semblable à celui de la protection de l'intégrité du noyau afin de prévenir les modifications du programme interne du coprocesseur. 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 gestion de la mémoire du coprocesseur de manière 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.

Le système d'exploitation du Secure Enclave est responsable de la configuration de la SCIP du Secure Enclave au démarrage.

Le matériel utilisé pour activer la SCIP est verrouillé après le processus de démarrage afin d'empêcher la reconfiguration. La SCIP est prise en charge par les puces-systèmes A12 et S4, et les plus récentes.

Codes d'authentification des pointeurs

Les codes d'authentification des pointeurs (PAC) sont utilisés pour empêcher l'exploitation des bogues d'altération de mémoire. Les logiciels système et les apps intégrées utilisent les PAC pour prévenir la modification des pointeurs de fonctions et des adresses de retour (pointeurs de code). Cela rend de nombreuses attaques plus difficiles. Par exemple, une attaque de programmation orientée retour (ROP) tente d'amener l'appareil à exécuter malicieusement un code existant en manipulant les adresses de retour des fonctions stockées sur la pile.

Les PAC sont pris en charge par les puces-systèmes A12 et S4.

Touch ID

Touch ID est le système de lecture d'empreintes digitales qui permet de sécuriser rapidement et facilement l'accès à l'iPhone ou à l'iPad. Cette technologie lit les données d'empreintes digitales sous n'importe quel angle et acquiert une meilleure connaissance de l'empreinte d'un utilisateur au fil du temps, le capteur continuant d'étendre la carte de l'empreinte à chaque fois qu'un nœud commun supplémentaire est détecté.

Face ID

En un clin d'œil, Face ID déverrouille en toute sécurité les appareils Apple qui sont dotés de cette fonctionnalité. Elle assure une authentification intuitive et sécurisée grâce au système de caméra TrueDepth doté de technologies avancées qui cartographient avec précision la géométrie de votre visage. Face ID utilise des réseaux neuronaux pour déterminer l'attention et la correspondance, et prévenir la mystification pour vous permettre de déverrouiller votre téléphone en un clin d'œil. Face ID s'adapte automatiquement aux changements de votre apparence et protège avec soin la confidentialité et la sécurité de vos données biométriques.

Touch ID, Face ID et les codes

Pour utiliser Touch ID ou Face ID, vous devez configurer votre appareil de sorte qu'un code soit nécessaire pour le déverrouiller. Lorsque Touch ID ou Face ID détecte une correspondance, votre appareil se déverrouille sans demander le code. Cela rend l'utilisation d'un code 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, mais elles facilitent l'accès à l'appareil tout en respectant des limites et des contraintes soigneusement réfléchies. Cet élément est important, car un code complexe constitue la base de la protection de vos données par chiffrement offerte par votre appareil iOS.

Vous pouvez utiliser votre code en tout temps à la place de Touch ID ou de Face ID, mais les opérations suivantes exigent toujours un code plutôt qu'un identificateur biométrique :

- la mise à jour de votre logiciel;
- l'effacement de votre appareil;
- l'affichage ou la modification des réglages du code;
- l'installation de profils de configuration iOS.

Un code est également requis si votre appareil se trouve dans les états suivants :

- l'appareil vient juste d'être allumé ou redémarré;
- l'appareil n'a pas été déverrouillé pendant plus de 48 heures;
- le code n'a pas été utilisé pour déverrouiller l'appareil au cours des 156 dernières heures (six jours et demi), et un identificateur biométrique n'a pas déverrouillé l'appareil au cours des quatre dernières heures;
- l'appareil a reçu une commande de verrouillage à distance;
- cinq tentatives infructueuses de mise en correspondance biométrique ont eu lieu;
- les fonctions Éteindre ou Urgence SOS ont été lancées.

Lorsque Touch ID ou Face ID est activé, l'appareil se verrouille dès que vous appuyez sur le bouton latéral et chaque fois qu'il se met en veille. Pour réactiver l'appareil après une mise en veille, Touch ID et Face ID doivent trouver une correspondance pour valider votre identité, ou vous devez entrer le code.

La probabilité qu'une personne choisie au hasard dans la population puisse déverrouiller votre iPhone 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 cinq empreintes et jusqu'à 1 sur 500 000 pour deux visages). Afin d'offrir

un niveau de protection supplémentaire, Touch ID et Face ID autorisent uniquement cinq tentatives infructueuses de mise en correspondance avant d'exiger le code pour déverrouiller votre appareil. 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. En cas de préoccupation à cet égard, Apple recommande l'utilisation d'un code pour l'authentification.

Sécurité de Touch ID

Le lecteur d'empreintes digitales n'est actif que lorsque l'anneau en acier capacitif qui entoure le bouton principal détecte le contact d'un doigt; la matrice d'imagerie avancée numérise alors l'empreinte et envoie l'image au Secure Enclave. La communication entre le processeur et le capteur Touch ID 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 prévue pour chaque capteur Touch ID et le coprocesseur Secure Enclave correspondant en usine. La clé partagée est complexe, aléatoire et différente pour chaque capteur Touch ID. L'échange de la clé de session se fait au moyen d'un **enveloppement de clé** AES, où les deux parties fournissent une clé aléatoire établissant la clé de session et utilisant le chiffrement AES-CCM pour le transport.

L'image tramée est stockée temporairement dans la mémoire chiffrée du Secure Enclave le temps d'être vectorisée en vue de son analyse, puis elle est effacée. L'analyse fait appel à une **cartographie des angles du flux des crêtes** sous-cutanées, un processus avec perte qui élimine les données de minuties nécessaires à la reconstruction de l'empreinte digitale réelle de l'utilisateur. La carte de nœuds ainsi obtenue est stockée sans informations d'identification dans un format chiffré qui ne peut être lu que 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.

Sécurité de Face ID

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.

La caméra TrueDepth cherche automatiquement votre visage lorsque vous réactivez un appareil Apple doté de Face ID en l'élevant ou en touchant l'écran ainsi que lorsque l'appareil tente de vous authentifier 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 vos yeux sont ouverts et que votre regard est dirigé vers celui-ci. Pour favoriser l'accessibilité, cette fonctionnalité 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 de votre visage 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 moteur neuronal des

puces-systèmes A11 et ultérieures, 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 de votre visage obtenue à partir d'une série de poses.

La mise en correspondance faciale est effectuée dans le Secure Enclave à l'aide de réseaux neuronaux conçus expressément à cette fin. Nous avons mis au point les réseaux neuronaux de correspondance faciale à l'aide de plus d'un milliard d'images, y compris des images infrarouges et tridimensionnelles recueillies lors d'études avec le consentement éclairé des participants. Apple a 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 élargies selon les besoins afin de fournir un degré de précision élevé pour un large éventail d'utilisateurs. Face ID a été conçue pour détecter les chapeaux, les lunettes, les verres de contact et de nombreuses lunettes de soleil. En outre, elle a été pensée pour fonctionner à l'intérieur, à l'extérieur et même dans l'obscurité totale. Un réseau neuronal supplémentaire conçu pour déceler la mystification et y résister vous protège contre les tentatives de déverrouillage de votre iPhone X à l'aide de photos ou de masques.

Les données de Face ID, y compris les représentations mathématiques de votre visage, 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 de votre visage calculées lors de la phase d'enregistrement;
- les représentations mathématiques de votre visage 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'enregistrement ou lors de comparaisons avec les données enregistrées de Face ID.

Comment Touch ID ou Face ID déverrouille un appareil iOS

Si Touch ID ou Face ID est désactivé, les clés de la classe la plus élevée de protection des données sont effacées lorsqu'un appareil se verrouille. Ces clés sont stockées dans le Secure Enclave. Les fichiers et les éléments du **trousseau** appartenant à cette classe restent inaccessibles jusqu'à ce que vous déverrouilliez l'appareil en entrant votre code.

Si Touch ID ou Face ID est activé, les clés ne sont pas effacées lorsque l'appareil 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. Lorsque vous tentez de déverrouiller l'appareil, si ce dernier détecte une correspondance, il fournit la clé permettant de développer les clés de protection des données. L'appareil est alors déverrouillé. 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 dont Touch ID et Face ID ont besoin pour le déverrouiller sont perdues. Elles sont effacées par le Secure Enclave lorsqu'une condition exigeant la saisie du code survient (par exemple lorsque l'appareil n'a pas été déverrouillé pendant 48 heures ou après cinq tentatives infructueuses de mise en correspondance).

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

Touch ID, Face ID, et Apple Pay

Vous pouvez 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. Pour en savoir plus sur Touch ID et Apple Pay, consultez la section « Apple Pay » du présent document.

Pour autoriser un paiement en magasin avec Face ID, vous devez d'abord confirmer votre intention de payer en appuyant deux fois sur le bouton latéral. Vous vous authentifiez ensuite avec Face ID avant de placer votre iPhone X à proximité du lecteur de paiement sans contact. Si vous souhaitez sélectionner un autre mode de paiement Apple Pay après l'authentification par Face ID, vous devrez vous authentifier de nouveau, mais vous n'aurez pas à réappuyer deux fois sur le bouton latéral.

Pour effectuer un paiement dans des apps ou sur le web, confirmez votre intention de payer en appuyant deux fois sur le bouton latéral, puis en vous authentifiant avec Face ID pour autoriser le paiement. Si votre transaction Apple Pay n'est pas terminée 30 secondes après que vous avez appuyé deux fois sur le bouton latéral, vous devrez confirmer de nouveau votre intention de payer en réappuyant deux fois sur le bouton.

Diagnostic Face ID

Les données de Face ID sont confinées dans votre appareil et ne sont jamais sauvegardées sur iCloud ni ailleurs. Ces informations ne sont transférées de votre appareil que dans le cas où vous souhaitez fournir des données de diagnostic Face ID à AppleCare pour obtenir de l'assistance. L'activation de Diagnostic Face ID nécessite une autorisation signée numériquement par Apple semblable à celle utilisée dans le cadre du processus de personnalisation de la mise à jour du logiciel. Une fois l'autorisation accordée, vous serez en mesure d'activer Diagnostic Face ID et de commencer le processus de configuration à partir de l'app Réglages des appareils qui prennent en charge Face ID.

Dans le cadre de la configuration de Diagnostic Face ID, votre enregistrement Face ID existant sera supprimé et vous devrez de nouveau enregistrer votre visage dans Face ID. Les appareils qui prennent en charge Face ID commenceront à enregistrer les images Face ID obtenues lors des

tentatives d'authentification pendant les dix jours suivants; ils arrêteront automatiquement d'enregistrer les images après cette période. Diagnostic Face ID n'envoie pas automatiquement les données à Apple. Vous pouvez examiner et approuver leur ajout, et déverrouiller les images (que les tentatives aient été fructueuses ou non) incluses dans les données de diagnostic de Face ID qui sont recueillies par le mode diagnostic avant de les envoyer à Apple. Diagnostic Face ID Diagnostics téléchargera uniquement les images que vous avez approuvées. Les données sont chiffrées avant le téléchargement, puis, une fois téléchargées, elles sont immédiatement supprimées. Les images que vous rejetez sont immédiatement supprimées.

Si vous ne terminez pas la session de Diagnostic Face ID en passant en revue les images et en téléchargeant celles que vous avez approuvées, la session prendra automatiquement fin après 40 jours, et toutes les images de diagnostic seront supprimées de l'appareil. Vous pouvez également désactiver Diagnostic Face ID en tout temps. Toutes les images locales seront alors immédiatement supprimées, et les données de Face ID ne seront pas partagées avec Apple.

Autres utilisations de Touch ID et de Face ID

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 ou d'un code. Les apps qui prennent en charge Touch ID prennent automatiquement en charge Face ID sans modification. Lorsque vous utilisez Touch ID ou Face ID, l'app n'est informée que de la réussite ou de l'échec de l'authentification; elle ne peut pas accéder à Touch ID, à Face ID ou aux données associées à l'utilisateur enregistré. 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 si le code de l'appareil est saisi. Les développeurs d'apps ont aussi à leur disposition des API qui permettent de vérifier si l'utilisateur a choisi un code et s'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 d'authentification d'API 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 ECC 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.

Vous pouvez également configurer Touch ID ou Face ID pour autoriser des achats dans l'iTunes Store, l'App Store et Apple Books, et ainsi éviter d'avoir à saisir le mot de passe d'un identifiant Apple. Sous iOS 11 ou toute version ultérieure, les clés ECC du Secure Enclave protégées par Touch ID ou Face ID sont utilisées pour autoriser les achats en signant la demande du commerçant.

Chiffrement et protection des données

Effacer contenu et réglages
L'option « Effacer contenu et réglages » de l'app Réglages efface toutes les clés présentes dans le stockage effaçable, rendant ainsi inaccessibles par chiffrement toutes les données d'utilisateur sur l'appareil. Il s'agit donc d'un moyen idéal pour s'assurer que toutes les données personnelles sont supprimées d'un appareil avant de transmettre ce dernier à quelqu'un d'autre ou de le faire réparer.

Important : N'utilisez jamais l'option « Effacer contenu et réglages » avant d'avoir effectué une sauvegarde de l'appareil, car il n'existe aucun moyen de récupérer les données effacées.

La chaîne de démarrage sécurisée, la signature du code et la sécurité des processus exécutés permettent de garantir que seuls le code et les apps fiables peuvent s'exécuter sur un appareil. iOS offre des fonctionnalités de chiffrement et de protection des données supplémentaires pour protéger les données utilisateur, même lorsque d'autres parties de l'infrastructure de sécurité ont été compromises (par exemple, sur un appareil sur lequel des modifications non autorisées ont été apportées). Cela apporte des avantages importants aussi bien pour les utilisateurs que pour les administrateurs informatiques, qui sont ainsi assurés que les informations personnelles et d'entreprise sont protégées à tout moment et disposent de méthodes d'effacement instantané et complet à distance en cas de vol ou de perte de l'appareil.

Fonctionnalités de sécurité matérielles

Sur les appareils mobiles, la vitesse et l'efficacité énergétique sont essentielles. Les opérations de chiffrement sont complexes et peuvent engendrer des problèmes de performances ou d'autonomie de la batterie si elles ne sont pas conçues et mises en œuvre en gardant ces priorités à l'esprit.

Chaque appareil iOS est doté d'un moteur de chiffrement AES 256 dédié intégré dans le chemin DMA entre le stockage flash et la mémoire principale du système, ce qui rend le chiffrement des fichiers extrêmement efficace. Sur les processeurs A9 ou toute version ultérieure de la série A, le système de stockage flash se trouve sur un bus isolé qui est uniquement autorisé à accéder à la mémoire contenant les données d'utilisateur par le moteur de chiffrement DMA.

L'identifiant unique (UID) et **l'identifiant de groupe (GID)** de l'appareil sont des clés AES 256 bits fusionnées (UID) ou compilées (GID) dans le processeur d'application et le Secure Enclave lors de la fabrication. Aucun logiciel ni programme interne ne peut les lire directement; ils ne peuvent voir que les résultats des opérations de chiffrement ou de déchiffrement réalisées par les moteurs AES dédiés implémentés dans le silicium à l'aide de l'UID ou du GID comme clé. Le processeur d'application et le Secure Enclave ont chacun leurs propres UID et GID. L'UID et le GID du Secure Enclave ne peuvent être utilisés que par le moteur AES qui y est dédié. Les UID et les GID ne sont pas non plus accessibles en passant par **Joint Test Action Group (JTAG)** ou d'autres interfaces de débogage.

À l'exception des puces-systèmes A8 et antérieures d'Apple, chaque Secure Enclave génère son propre UID au cours du processus de fabrication. Puisque l'UID est propre à chaque appareil et qu'il est généré entièrement dans le Secure Enclave plutôt que dans un système de fabrication à l'extérieur de l'appareil, l'UID n'est pas accessible et ne peut pas être stocké par Apple ou ses fournisseurs.

Le logiciel exécuté sur le Secure Enclave profite de 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 inclut l'UID; ainsi, si les puces de mémoire sont transférées d'un appareil à un autre, les fichiers sont inaccessibles. L'UID n'est lié à aucun autre identifiant sur l'appareil.

Les GID sont communs à tous les processeurs d'une même classe d'appareils (par exemple tous les appareils dotés du processeur A8 d'Apple).

À part l'UID et le GID, toutes les autres clés de chiffrement sont créées par le générateur de nombres aléatoires (RNG) du système à l'aide d'un algorithme basé sur le code source CTR_DRBG. L'entropie du système est générée à partir de variations de synchronisation lors du démarrage et à partir d'une synchronisation par interruption une fois l'appareil démarré. Les clés générées à l'intérieur de la puce du Secure Enclave utilisent son générateur matériel de nombres véritablement aléatoires basé sur plusieurs oscillateurs en anneau post-traités avec CTR_DRBG.

L'effacement sécurisé des clés enregistrées est tout aussi important que leur génération. Cela s'avère particulièrement délicat dans le stockage flash, par exemple lorsque le contrôle d'usure peut nécessiter l'effacement de plusieurs copies des données. Pour traiter ce problème, les appareils iOS intègrent une fonctionnalité dédiée à l'effacement sécurisé des données appelée **Stockage effaçable**. Cette fonctionnalité accède à la technologie de stockage sous-jacente (par exemple, NAND) pour effacer directement un petit nombre de blocs à un niveau très bas.

Cartes Express avec réserve d'énergie

Si iOS n'est pas en marche parce que l'iPhone doit être chargé, il se peut qu'il reste assez d'énergie dans la batterie pour prendre en charge les transactions de cartes Express.

Les iPhone compatibles prennent automatiquement en charge cette fonctionnalité avec :

- une carte de transport désignée comme carte de transport en commun Express;
- les cartes étudiantes dont le mode Express est activé.

Appuyer sur le bouton latéral affiche l'icône de batterie faible ainsi qu'un message indiquant que les cartes Express sont utilisables. Le contrôleur NFC exécute les transactions de cartes Express selon les mêmes conditions que lorsqu'iOS est en marche, mais les transactions sont signalées uniquement par une vibration. Aucune notification visible ne s'affiche.

Cette fonctionnalité n'est pas disponible lorsque l'appareil a été éteint normalement par l'utilisateur.

Protection des données des fichiers

En plus des fonctionnalités de chiffrement matérielles intégrées aux appareils iOS, Apple utilise une technologie appelée Protection des données pour accroître la protection des données stockées dans la mémoire flash de l'appareil. 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. Les apps clés du système, comme Messages, Mail, Calendrier, Contacts, Photos et les données Santé, utilisent par défaut la protection des données, et les apps tierces installées sur iOS 7 ou version ultérieure bénéficient automatiquement de cette protection.

La protection des données est mise en œuvre en élaborant et en gérant une hiérarchie de clés, et repose sur les technologies de chiffrement matérielles intégrées à chaque appareil iOS. Elle est contrôlée fichier par fichier en attribuant une classe à chacun d'eux; l'accessibilité est déterminée par le déverrouillage des clés de classe. Avec l'arrivée du système de fichiers d'Apple (APFS), il est désormais possible de subdiviser les clés par domaine (les parties d'un fichier peuvent avoir différentes clés).

Vue d'ensemble de l'architecture

Chaque fois qu'un fichier est créé sur la partition de données, la protection des données crée une nouvelle clé 256 bits (la clé « par fichier ») et la transmet au moteur AES matériel, qui l'utilise alors pour chiffrer le fichier lors de son écriture dans la mémoire flash en utilisant le mode AES XTS. Sur les appareils dotés d'une puce-système A7, S2 ou S3, le mode AES-CBC est utilisé. Le vecteur d'initialisation est calculé avec le décalage de bloc du fichier, chiffré avec le hachage SHA-1 de la **clé par fichier**.

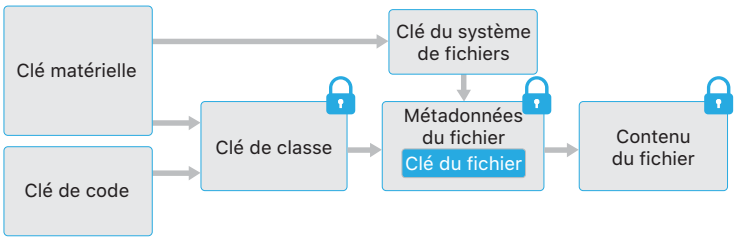
La clé par fichier (ou par domaine) est enveloppée avec une des clés de classe, selon les circonstances dans lesquelles le fichier doit être accessible. Comme tous les autres enveloppements, celui-ci est réalisé à l'aide de l'enveloppement de clé AES NIST, selon RFC 3394. La clé par fichier enveloppée 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 seront 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 développée à l'aide de la clé de classe, puis transmise au moteur AES matériel, qui déchiffre le fichier lors de sa lecture à partir de la mémoire flash. Toute la gestion des clés de fichier enveloppées se produit 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 développe les clés d'un fichier, ces dernières sont enveloppées de nouveau avec la clé éphémère, puis renvoyées au processeur d'application.

Les métadonnées de tous les fichiers présents dans le système de fichiers sont chiffrées avec une clé aléatoire, qui est créée lors de l'installation initiale d'iOS ou lors de l'effacement du contenu de l'appareil par l'utilisateur. Sur les appareils qui prennent en charge l'APFS, la clé de métadonnées du système de fichiers est enveloppée par la clé UID pour le stockage à long terme. Tout comme les clés par fichier ou par domaine, la clé de métadonnées n'est jamais exposée directement au processeur d'application; le Secure Enclave fournit plutôt une version éphémère par démarrage. Lorsqu'elle est stockée, la clé du système de fichiers chiffrée est aussi enveloppée par une « clé effaçable » stockée dans le stockage effaçable. Cette clé n'augmente 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 émettant une commande d'effacement à distance à partir d'une solution de GAM, d'Exchange ActiveSync ou d'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 du matériel et, pour certaines classes, le code de l'utilisateur. Cette hiérarchie offre à la fois souplesse et performances. Par exemple, changer la classe d'un fichier peut se faire simplement en enveloppant à nouveau sa clé par fichier, et la modification du code ne réenveloppe que la clé de classe.

Codes

En définissant un code d'appareil, l'utilisateur active automatiquement la protection des données. iOS prend en charge les codes alphanumériques à six chiffres, à quatre chiffres et à longueur arbitraire. En plus de déverrouiller l'appareil, un code fournit l'entropie pour certaines clés de chiffrement. Cela signifie qu'une personne malintentionnée en possession d'un appareil ne peut pas accéder aux données appartenant à des classes de protection précises sans le code.

Le code étant combiné à l'UID de l'appareil, des attaques en force sont nécessaires pour tenter d'accéder à celui-ci. 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. Ainsi, il faudrait plus de cinq ans et demi pour essayer toutes les combinaisons d'un code alphanumérique à six caractères composé de minuscules et de chiffres.

Plus le code de l'utilisateur est complexe, plus la clé de chiffrement l'est également. Touch ID et Face ID peuvent être utilisés pour renforcer cette équation en permettant à l'utilisateur de choisir un code beaucoup plus compliqué qu'il ne le ferait en temps normal pour des raisons pratiques. Cela augmente le degré réel d'entropie protégeant les clés de chiffrement utilisées pour la protection des données sans avoir d'impact négatif sur l'expérience de l'utilisateur qui déverrouille son appareil iOS plusieurs 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 de verrouillage. Si l'option Réglages > Touch ID et code > Effacer les données est activée, l'appareil efface automatiquement les données après dix tentatives infructueuses consécutives de saisie du code. 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 GAM qui prend en charge cette fonctionnalité et Exchange ActiveSync, de même qu'être fixé à un seuil inférieur.

Remarques à propos du code
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.

Délais entre tentatives de code

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

Accès au mode de mise à niveau du logiciel interne d'un appareil (DFU) 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 que du code intact signé Apple. Le mode DFU est accessible manuellement.

Connectez d'abord l'appareil à un ordinateur à l'aide d'un câble USB.

Puis, selon l'appareil, effectuez ce qui suit :

iPhone X ou modèle plus récent, iPhone 8 ou iPhone 8 Plus. Appuyez sur le bouton de volume du haut et relâchez-le rapidement. Appuyez sur le bouton de volume du bas et relâchez-le rapidement. Appuyez de façon prolongée sur le bouton latéral, puis appuyez de nouveau sur le bouton de volume du bas. Après 5 secondes, relâchez le bouton latéral et continuez d'appuyer sur le bouton de volume du bas jusqu'à ce que vous voyiez un écran noir.

iPhone 7 ou iPhone 7 Plus. Maintenez le bouton latéral et le bouton de volume du bas enfoncés en même temps. Après 8 secondes, relâchez le bouton latéral et continuez d'appuyer sur le bouton de volume du bas jusqu'à ce que vous voyiez un écran noir.

iPhone 6s ou modèle précédent, iPad ou iPod touch. Maintenez le bouton principal et le bouton du haut (ou latéral) enfoncés en même temps. Après 5 secondes, relâchez le bouton du haut (ou latéral) et continuez d'appuyer sur le bouton principal jusqu'à ce que vous voyiez un écran noir.

Apple TV. Connectez votre appareil à votre ordinateur avec un câble Micro-USB, puis forcez l'appareil à redémarrer en maintenant le bouton de menu et le bouton du bas enfoncés en même temps pendant 6 à 7 secondes. Immédiatement après le redémarrage, appuyez simultanément sur Menu et Lecture jusqu'à ce qu'un message s'affiche dans iTunes, indiquant la détection d'une Apple TV en mode de récupération.

Remarque : Rien ne s'affiche à l'écran lorsque l'appareil est en mode DFU. Si le logo Apple apparaît, c'est que le bouton latéral ou de mise en veille a été maintenu enfoncé trop longtemps. Si le passage de l'appareil en mode DFU a réussi, l'écran sera noir et iTunes affichera un message indiquant : « iTunes a détecté un (iPad, iPhone ou iPod touch) en mode de récupération. Vous devez restaurer cet appareil (iPad, iPhone ou iPod touch) avant de pouvoir l'utiliser avec iTunes. »

Sur les appareils dotés du coprocesseur Secure Enclave, les délais sont imposés par ce dernier. Si l'appareil est redémarré au cours du décompte d'un délai, ce dernier reste imposé, la minuterie reprenant son cours.

Pour améliorer la sécurité tout en préservant la convivialité, Touch ID, Face ID ou le code de sécurité est requis pour établir une connexion via un accessoire Lightning, USB ou Smart Connector si aucune connexion n'a été établie récemment. 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 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. Si un accessoire inconnu tente d'établir une connexion avec les données pendant cette période, toutes les connexions (Lightning, USB et Smart Connector) sont désactivées jusqu'à ce que l'appareil soit de nouveau déverrouillé.

Cette période d'une heure :

- permet de 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.

En outre, 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.

Mode DFU et mode de récupération

Sur les appareils dotés d'une puce-système A10, A11 ou S3 d'Apple, les clés de classe protégées par le code de l'utilisateur ne sont pas accessibles à partir du mode de récupération. Les puces-systèmes A12 et S4 offrent également cette protection en mode DFU.

Le moteur AES du Secure Enclave est équipé de bits logiciels de départ 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.

À partir des puces-systèmes 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 ou 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 puces-systèmes 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 prévient l'accès aux données protégées par le code de l'utilisateur.

Sur les puces-systèmes A10, A11, S3 et S4 d'Apple, le bit de départ du code est verrouillé par le système d'exploitation du Secure Enclave si l'appareil passe en mode de récupération. La mémoire morte d'amorçage et le système d'exploitation du Secure Enclave vérifient tous les deux le registre de progression du démarrage pour déterminer sécuritairement le mode actuel.

Classes de protection des données

Lorsqu'un fichier est créé sur un appareil iOS, l'app qui le crée lui attribue une classe. 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.

Protection complète

`(NSFileProtectionComplete)` : la clé de classe est protégée par une clé obtenue à partir du code de l'utilisateur et de l'UID de l'appareil. Peu après le blocage de l'appareil par l'utilisateur (dix secondes si le réglage Exiger le mot de passe est réglé sur Immédiatement), la clé de classe déchiffrée est abandonnée, rendant ainsi l'intégralité des données de la classe inaccessibles jusqu'à ce que l'utilisateur ressaisisse le code ou déverrouille l'appareil à l'aide de Touch ID ou de Face ID.

Protection complète sauf si des données sont ouvertes

`(NSFileProtectionCompleteUnlessOpen)` : il peut arriver que des fichiers doivent être écrits pendant le verrouillage de l'appareil. Cela est le cas, par exemple, lors du téléchargement d'une pièce jointe en arrière-plan. Ce comportement est obtenu grâce à la cryptographie asymétrique à courbes elliptiques (ECDH sur Curve25519). La clé par fichier habituelle est protégée par une clé obtenue au moyen de l'accord de clé Diffie-Hellman à une passe, comme décrit dans la norme NIST SP 800-56A.

La clé publique éphémère de l'accord est stockée avec la clé par fichier enveloppée. KDF est la fonction de dérivation des clés de concaténation (solution approuvée 1) telle que décrite dans la section 5.8.1 de la norme NIST SP 800-56A. AlgorithmID est omis. PartyUInfo et PartyVInfo correspondent respectivement aux clés publiques éphémère et statique. SHA-256 est utilisée comme fonction de hachage. 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 Protected Unless Open (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 est utilisée pour déchiffrer le fichier.

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

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

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.

Clé de classe de protection des données

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	(NSFileProtectionCompleteUntilFirstUserAuthentication)
Classe D	Aucune protection	(NSFileProtectionNone)

Composants d'un élément de trousseau

En plus du groupe d'accès, chaque élément de trousseau contient des métadonnées administratives (comme une date de création et une date de dernière modification).

Il contient également des hachages SHA-1 des attributs utilisés pour obtenir l'élément (comme le nom du compte et le nom du serveur). Ceci permet d'exécuter une recherche sans devoir déchiffrer chaque élément. Enfin, il contient les données de chiffrement, qui incluent les informations suivantes :

- numéro de version;
- données de liste de contrôle d'accès (ACL);
- valeur indiquant la classe de protection à laquelle appartient l'élément;
- clé d'élément enveloppée dans la clé de classe de protection;
- dictionnaire d'attributs décrivant l'élément (tel que transmis à SecItemAdd), encodé en tant que fichier plist binaire et chiffré avec la clé d'élément.

Le chiffrement est de type AES-256 en mode GCM (Galois/Counter); le groupe d'accès est inclus dans les attributs et protégé par le code GMAC calculé pendant le chiffrement.

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 session. Le trousseau iOS offre un moyen sûr de stocker ces éléments.

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 la recherche alors que la valeur secrète (kSecValueData) est chiffrée avec la clé secrète. La clé de métadonnées est protégée par le processeur 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 processeur 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 application 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. Cette restriction est mise en œuvre en obligeant les apps tierces à utiliser des groupes d'accès portant un préfixe qui leur est alloué par le programme Apple pour les développeurs par l'intermédiaire des 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 qu'elles utilisent sont différentes, tout comme les noms des API auxquelles elles sont intégrées.

Disponibilité	Protection des données des fichiers	Protection des données du trousseau
Lorsque l'appareil est déverrouillé	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
Lorsque l'appareil est verrouillé	NSFileProtectionCompleteUnlessOpen	N/D
Après le premier déverrouillage	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Toujours	NSFileProtectionNone	kSecAttrAccessibleAlways
Code activé	N/D	kSecAttrAccessible WhenPasscodeSetThisDeviceOnly

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 dépôt.

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 facilité d'utilisation en choisissant les classes du trousseau qui dépendent du type d'informations sécurisées et en définissant quand elles sont requises par iOS. 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.

Pour les éléments du trousseau créés par iOS, les protections de classe suivantes sont appliquées :

Élément	Accessible
Mots de passe Wi-Fi	Après le premier déverrouillage
Comptes Mail	Après le premier déverrouillage
Comptes Exchange	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
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 iTunes	Lorsque l'appareil est déverrouillé, non itinérant
Certificats VPN	Toujours, non itinérant
Clés Bluetooth®	Toujours, non itinérant
Jeton du service de notifications Push d'Apple (APN)	Toujours, non itinérant
Certificats et clé privée iCloud	Toujours, non itinérant
Clés iMessage	Toujours, non itinérant
Clés privées et certificats installés par un profil de configuration	Toujours, non itinérant
Code NIP de la carte SIM	Toujours, non itinérant
Jeton Localiser mon iPhone	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 de Face ID, ou en saisissant le code de l'appareil. Il est aussi possible de limiter l'accès aux éléments en indiquant que l'enregistrement Touch ID ou Face ID n'a pas changé depuis l'ajout de l'élément. Cette limite contribue à empêcher une personne malintentionnée 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.

Conteneurs de clés

Les clés des classes de protection des données, pour les fichiers et le trousseau, sont rassemblées et gérées dans des conteneurs de clés. iOS utilise les conteneurs de clés suivants : utilisateur, appareil, sauvegarde, dépôt et sauvegarde iCloud.

Le **conteneur de clés de l'utilisateur** est l'endroit où les clés de classe enveloppées utilisées lors du fonctionnement normal de l'appareil sont stockées. Par exemple, lorsqu'un code est saisi, la clé `NSFileProtectionComplete` est chargée à partir du conteneur de clés du système et développée. Il s'agit d'un fichier binaire de liste de propriétés (.plist) appartenant à la classe Aucune protection, mais dont le contenu est chiffré à l'aide d'une clé conservée 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. L'extension du noyau `AppleKeyStore` gère le conteneur de clés de l'utilisateur et peut être interrogée sur l'état de verrouillage d'un appareil. Elle 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 développées.

Le **conteneur de clés de l'appareil** sert à stocker les clés de classe enveloppées utilisées pour les opérations faisant appel à des données spécifiques à l'appareil. Les appareils iOS configurés pour un usage partagé ont parfois besoin d'accéder à des informations d'identification pour qu'un utilisateur puisse ouvrir sa session. Dès lors, un conteneur de clés qui n'est pas protégé par le code de l'utilisateur devient obligatoire. iOS ne prend pas en charge la distance 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 pour chaque 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 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.

Le conteneur de clés de sauvegarde est créé lorsqu'iTunes 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.

Le conteneur de clés est protégé par le mot de passe défini dans iTunes, soumis à dix millions d'itérations de 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 complexe.

Si un utilisateur choisit de ne pas chiffrer une sauvegarde iTunes, les fichiers de sauvegarde 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.

Le conteneur de clés de dépôt est utilisé pour la synchronisation iTunes et par les solutions de gestion des appareils mobiles (GAM). Ce conteneur de clés permet 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 iTunes, ou dans la solution de GAM qui gère l'appareil à distance.

Le conteneur de clés de dépôt 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 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 dépôt contenant les mêmes clés de classe que celles qu'il utilise et génère une nouvelle clé pour le protéger. Le conteneur de clés de dépôt 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 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 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.

L'incrémentation du compteur de jetons de déverrouillage à usage unique dans le Secure Enclave invalide tout jeton existant. Le compteur est incrémenté lorsqu'un jeton est utilisé, après le premier déverrouillage d'un appareil redémarré, lorsqu'une mise à jour logicielle est annulée (par l'utilisateur ou par le système) ou quand la minuterie du règlement d'un jeton a expiré.

Le jeton de déverrouillage à usage unique pour les mises à jour logicielles surveillées expire au bout de 20 minutes. Ce jeton est exporté à partir du Secure Enclave et il est écrit sur un espace de stockage effaçable. La minuterie d'un 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 que :

- les mises à jour automatiques sont configurées dans iOS 12 (ou une version ultérieure);

  ou

- l'utilisateur choisit « Installer plus tard » lorsqu'il en est informé.

Une fois que l'utilisateur saisit son code, un jeton de déverrouillage à usage unique est généré et il 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.

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 étant asymétriques (utilisation de Curve25519, comme la classe de protection de données Protection complète sauf si des données sont ouvertes), les sauvegardes iCloud peuvent être réalisées en arrière-plan. Pour toutes les classes de protection des données, à l'exception d'Aucune Protection, les données chiffrées sont lues sur l'appareil et envoyées à iCloud. Les clés de classe correspondantes sont protégées par des clés iCloud. Les clés de classe du trousseau sont enveloppées avec une clé dérivée de l'UID comme lors d'une sauvegarde iTunes non chiffrée. Un conteneur de clés asymétriques est également utilisé pour la sauvegarde dans la fonctionnalité de récupération du trousseau iCloud.

Sécurité des apps

Les apps sont parmi les éléments les plus critiques d'une architecture de sécurité mobile moderne. Bien qu'elles apportent d'incroyables avantages aux utilisateurs en matière de productivité, elles sont aussi susceptibles d'avoir un effet négatif sur la sécurité du système, sa stabilité et les données utilisateur si elles ne sont pas correctement gérées.

C'est pourquoi iOS est doté de couches de protection chargées de s'assurer que les apps sont signées et vérifiées, et de les placer dans un bac à sable pour protéger les données utilisateur. Ces éléments fournissent une plateforme stable et sécurisée pour les apps, ce qui permet à des milliers de développeurs de proposer des centaines de milliers d'apps sur iOS sans incidence sur l'intégrité du système. Et les utilisateurs peuvent accéder à ces apps sur leur appareil iOS sans craindre outre mesure les virus, les logiciels malveillants ou autres attaques non autorisées.

Signature du code des apps

Après son démarrage, le noyau iOS contrôle les apps et processus utilisateur autorisés à s'exécuter. Pour garantir que toutes les apps proviennent d'une source connue et approuvée et qu'elles n'ont pas été altérées, iOS exige 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 empêche les apps de tiers de charger du code non signé ou d'utiliser du code susceptible de se modifier de façon autonome.

Pour pouvoir développer et installer des apps sur des appareils iOS, les développeurs doivent s'inscrire auprès d'Apple et adhérer au programme Apple pour les développeurs. L'identité réelle de chaque développeur, qu'il s'agisse d'un particulier ou d'une entreprise, est vérifiée par Apple avant l'émission de son certificat. Ce certificat permet aux développeurs de signer des apps et de les soumettre à l'App Store en vue de leur distribution. Toutes les apps disponibles dans l'App Store sont donc proposées par des personnes et des entreprises identifiables, ce qui dissuade les développeurs de créer des apps malveillantes. Elles sont également vérifiées par Apple afin de s'assurer qu'elles fonctionnent comme décrites et ne présentent pas de bogues évidents ni d'autres problèmes. En plus des technologies déjà abordées, ce processus de sélection garantit aux clients la qualité des apps qu'ils achètent.

iOS permet 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'adresse, 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 (Team ID) issu d'un certificat émis par Apple. Un identifiant

d'équipe est une chaîne alphanumérique comportant dix 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.

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 organismes 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'un organisme est membre de l'ADEP, il 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 garantit que seuls les utilisateurs prévus de l'organisme peuvent charger les apps sur leurs appareils iOS. Les apps installées à l'aide de la GAM sont considérées implicitement comme fiables, car la relation entre l'entreprise et l'appareil est déjà établie. À défaut, 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.

Contrairement aux autres plateformes mobiles, iOS n'autorise pas les utilisateurs à installer des apps non signées potentiellement malveillantes à partir de sites web ni à exécuter du code non approuvé. Lors de l'exécution, des contrôles de signature du code des pages mémoire de tous les exécutables sont réalisés au fil de leur chargement pour s'assurer qu'une app n'a pas été modifiée depuis son installation ou sa dernière mise à jour.

Sécurité des processus exécutés

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

Toutes les apps de tiers sont placées dans un 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 empêche 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 de tiers doit accéder à des informations autres que les siennes, elle ne peut le faire qu'en utilisant les services explicitement fournis par iOS.

Les fichiers et ressources du système sont également protégés des apps de l'utilisateur. La majeure partie d'iOS s'exécute en tant qu'utilisateur non privilégié « mobile », comme toutes les apps de tiers. L'ensemble de la partition du système d'exploitation est monté en lecture seule. Les outils qui ne sont pas indispensables, comme les services d'ouverture de session 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 l'iOS.

L'accès aux informations de l'utilisateur et à des fonctionnalités comme iCloud et l'extensibilité par les apps de tiers sont contrôlés à l'aide de déclarations d'autorisation. Les déclarations d'autorisation sont des paires de valeurs clés signées intégrées à une app et permettent l'authentification au-delà des facteurs d'exécution, comme l'identifiant utilisateur UNIX. Comme les déclarations d'autorisation sont signées numériquement, elles ne peuvent pas être modifiées. Les déclarations d'autorisation sont très utilisées par les apps et les démons système pour réaliser des opérations nécessitant des privilèges spécifiques pour lesquelles le processus devrait normalement s'exécuter en tant qu'utilisateur root. Cela réduit considérablement le risque d'augmentation des privilèges par une app ou un démon système compromis.

En outre, les apps ne peuvent réaliser un traitement en arrière-plan que par le biais 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.

Le **protocole de distribution aléatoire de l'espace d'adressage (ASLR)** empêche l'exploitation des bogues d'altération de mémoire. Les apps intégrées utilisent l'ASLR pour garantir la distribution aléatoire de toutes les régions 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 sophistiqués. Par exemple, une attaque de type return-to-libc tente d'amener un appareil à exécuter un code malveillant en manipulant les adresses mémoire des bibliothèques de pile et système. L'organisation aléatoire de celles-ci rend l'attaque beaucoup plus difficile à exécuter, en particulier sur plusieurs appareils. Xcode, l'environnement de développement d'iOS, compile automatiquement les programmes tiers avec la prise en charge de l'ASLR activée.

Une protection supplémentaire est apportée par iOS 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 du droit de signature de code dynamique réservé à Apple. Même dans ce cas, un seul appel mmap est autorisé pour demander une page exécutable et accessible en écriture, qui se voit attribuer une adresse aléatoire. Safari utilise cette fonctionnalité pour son compilateur JavaScript JIT.

Extensions

iOS permet à des apps d'étendre les fonctionnalités d'autres apps par le biais d'extensions. Incorporées dans une app, les extensions sont des exécutables binaires signés ayant une fonction spéciale. Le système détecte automatiquement les extensions lors de l'installation et les rend accessibles aux autres apps à l'aide d'un système de mise en correspondance.

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 les widgets Aujourd'hui, Partager, les actions Personnalisé, Édition photo, Fournisseur de documents et Clavier personnalisé.

Les extensions s'exécutent dans leur propre espace d'adresse. La communication entre une extension et l'app à partir de laquelle elle a été activée se fait par le biais des communications interprocessus assistées par le cadre d'application système. Elles n'ont pas accès aux fichiers ni aux espaces mémoire de l'autre. Les extensions sont conçues pour être isolées l'une de l'autre, de l'app qui les contient et des apps qui les utilisent. Elles sont placées dans un bac à sable comme toute autre app de tiers et possèdent un conteneur distinct de celui de l'app. Toutefois, elles partagent le même accès aux contrôles de confidentialité que cette dernière. 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.

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 présentation sécurisée. Pour limiter le transfert des données d'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.

Pour les appareils inscrits à une solution de GAM, les extensions de document et de clavier obéissent aux règles de gestion d'ouverture de fichier (Managed Open In). Par exemple, la solution de GAM peut empêcher un utilisateur 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.

Groupes 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 garantit que les identifiants de groupe d'apps sont uniques dans l'ensemble de l'écosystème d'apps.

Protection des données dans les apps

Le kit de développement de logiciels (SDK, Software Development Kit) pour iOS offre une suite complète 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.

Accessoires

Le programme d'homologation « Conçu pour » 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 à l'aide d'un connecteur Lightning 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) personnalisé 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; par exemple, l'accès à des flux audio numériques sur le câble Lightning ou à des informations de localisation fournies par Bluetooth. Un CI d'authentification garantit 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 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).

HomeKit

HomeKit fournit une infrastructure d'automatisation à domicile qui fait appel aux fonctionnalités de sécurité d'iCloud et d'iOS pour protéger et synchroniser les données personnelles sans les exposer à Apple.

Identité HomeKit

La sécurité et l'identité HomeKit reposent sur des paires de clés publiques-privées Ed25519. Une paire de clés Ed25519 est générée pour HomeKit sur l'appareil iOS pour chaque utilisateur et devient son identité HomeKit. Elle est utilisée pour authentifier la communication entre les appareils iOS, et entre les appareils iOS et les accessoires.

Les clés sont stockées dans le trousseau et incluses uniquement dans les sauvegardes chiffrées de ce dernier. Elles sont synchronisées entre les appareils à l'aide du trousseau iCloud, le cas échéant. Le HomePod et l'Apple TV reçoivent des clés par l'intermédiaire 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 par l'intermédiaire du service d'identité Apple (IDS).

Communication avec les accessoires HomeKit

Les accessoires HomeKit génèrent leur propre paire de clés Ed25519 pour communiquer avec les appareils iOS. 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 et un accessoire HomeKit, les clés sont échangées à l'aide du protocole Secure Remote Password (3 072 bits), en utilisant un code à huit chiffres fourni par le fabricant de l'accessoire et saisi sur l'appareil iOS par l'utilisateur, puis chiffré avec l'algorithme AEAD CHACHA20-POLY1305 avec des clés obtenues à l'aide de la fonction de dérivation HKDF-SHA-512. La certification MFi de l'accessoire est également vérifiée lors de la configuration. Les accessoires sans puce MFi peuvent intégrer la prise en charge de l'authentification logicielle sous iOS 11.3 ou ultérieur.

Lorsque l'appareil iOS et l'accessoire HomeKit communiquent, chacun authentifie l'autre en utilisant les clés échangées comme décrites ci-dessus. Chaque session est établie à l'aide du protocole Station-to-Station et chiffrée avec les clés obtenues à l'aide de la fonction de dérivation HKDF-SHA-512 à partir des clés Curve25519 par session. Cela s'applique aux accessoires IP et aux accessoires Bluetooth Low Energy.

Pour les appareils Bluetooth Low Energy qui prennent en charge les notifications de diffusion, l'accessoire reçoit une clé de diffusion de la part d'un appareil iOS 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 annonces Bluetooth Low Energy. La clé de chiffrement de diffusion est une clé obtenue à l'aide de la fonction de dérivation HKDF-SHA-512 et les données sont chiffrées à l'aide de l'algorithme de chiffrement authentifié avec données associées (AEAD) CHACHA20-POLY1305. La clé de chiffrement de diffusion est régulièrement modifiée par l'appareil iOS et synchronisée avec les autres appareils à l'aide d'iCloud comme décrit dans la section « Synchronisation des données entre les appareils et les utilisateurs » ci-dessous.

Stockage local des données

HomeKit stocke les données concernant les domiciles, les accessoires, les scènes et les utilisateurs sur l'appareil iOS 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 ne sont sauvegardées que dans des sauvegardes chiffrées; ainsi, les sauvegardes iTunes non chiffrées, par exemple, ne contiennent pas les données HomeKit.

Synchronisation des données entre les appareils et les utilisateurs

Les données HomeKit peuvent être synchronisées entre les appareils iOS d'un utilisateur à l'aide d'iCloud et du trousseau iCloud. Les données HomeKit sont chiffrées pendant la synchronisation à l'aide de clés obtenues à partir de l'identité HomeKit de l'utilisateur et d'un nonce aléatoire. Ces données sont traitées sous la forme d'un blob opaque pendant la synchronisation. Le blob le plus récent est stocké dans iCloud pour permettre la synchronisation, 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 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 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 par session.

L'utilisateur ayant initialement créé le domicile dans HomeKit ou un autre utilisateur ayant des autorisations de modification peuvent ajouter des utilisateurs. L'appareil du propriétaire configure les accessoires avec la clé publique du nouvel utilisateur afin qu'ils puissent authentifier et accepter les commandes de ce dernier. Lorsqu'un utilisateur qui dispose d'autorisations de modification ajoute un nouvel utilisateur, le processus est délégué à un concentrateur Domicile pour conclure l'opération.

Le processus pour approvisionner l'Apple TV et l'utiliser avec HomeKit est effectué automatiquement 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 au moyen d'iCloud. Lorsque 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 par session. Ce processus fait appel à une authentification et à un chiffrement identiques à ceux utilisés entre un appareil iOS et un accessoire HomeKit. L'appareil du propriétaire transfère les paires de clés publiques-privées Ed25519 vers l'Apple TV au moyen de 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 qui appartiennent au domicile HomeKit.

Si un utilisateur n'a qu'un seul appareil et qu'il refuse d'accorder l'accès à son domicile à d'autres utilisateurs, aucune donnée HomeKit n'est synchronisée avec iCloud.

Données du domicile et apps

L'accès aux données du domicile par les apps 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. 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 suivante : https://developer.apple.com/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 endroits 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. Pour en savoir plus, consultez la sous-section « Siri » de la section « Services internet » du présent document.

Caméras IP HomeKit

Dans HomeKit, les caméras IP envoient des flux vidéo et audio directement à l'appareil iOS connecté au réseau local y ayant accès. Les flux sont chiffrés à l'aide de clés générées aléatoirement sur l'appareil iOS et la caméra IP, qui sont échangées au moyen de la session HomeKit sécurisée donnant accès à la caméra. Lorsque l'appareil iOS n'est pas connecté au réseau local, les flux chiffrés lui sont relayés par le concentrateur. Le concentrateur ne déchiffre pas les flux et sert simplement de relais entre l'appareil iOS et la caméra IP. Lorsqu'une app affiche l'image vidéo de la caméra IP HomeKit à l'attention de l'utilisateur, HomeKit assure sa conversion sécurisée à partir d'un processus système séparé de façon à ce que l'app ne puisse pas accéder ou stocker le flux vidéo. En outre, les apps ne sont pas autorisées à saisir des captures d'écran de ce flux.

Accès distant à iCloud pour les accessoires HomeKit

Un accessoire HomeKit peut se connecter directement à iCloud pour permettre aux appareils iOS de le contrôler si les transmissions par Bluetooth ou par Wi-Fi ne sont pas disponibles.

L'accès distant à iCloud a été soigneusement conçu pour que les accessoires puissent être contrôlés et des notifications envoyées sans révéler à Apple l'identité des accessoires ou les commandes et notifications envoyées. HomeKit n'envoie pas d'informations relatives au domicile à travers l'accès distant à iCloud.

Lorsqu'un utilisateur envoie une commande par le biais de l'accès distant à iCloud, l'accessoire et l'appareil iOS sont mutuellement authentifiés et les données sont chiffrées en utilisant la même procédure décrite pour les connexions locales. Le contenu des transmissions est chiffré et n'est pas visible par Apple. L'adressage à travers iCloud s'articule autour d'identifiants iCloud inscrits au cours du processus de configuration.

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 l'ouverture d'une session de l'utilisateur sur iCloud. L'appareil iOS demande ensuite à l'accessoire de signer un défi en utilisant le coprocesseur d'authentification d'Apple, intégré dans tous les accessoires conçus pour HomeKit. L'accessoire génère également des clés elliptiques de type prime256v1, et la clé publique est envoyée à l'appareil iOS 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 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 distant à iCloud. Ces informations ne sont pas spécifiques à un utilisateur ni à un accessoire particulier.

Chaque accessoire inscrit une liste d'utilisateurs autorisés auprès du serveur d'accès distant à iCloud. Ces utilisateurs se voient accorder le droit de contrôler l'accessoire par la personne ayant ajouté l'accessoire au domicile. Le serveur iCloud affecte un identifiant aux utilisateurs, qu'il est possible d'associer à un compte iCloud dans le but de distribuer les messages de notification et les réponses des accessoires. De même, les accessoires possèdent un identifiant émis par iCloud, mais qui est opaque et ne révèle aucune information relative à l'accessoire même.

Lorsqu'un accessoire se connecte au serveur d'accès distant à iCloud pour HomeKit, il présente son certificat et un billet. Ce billet est obtenu auprès d'un serveur iCloud différent; celui-ci n'est pas unique 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. La connexion au serveur de billet n'est pas authentifiée afin de contribuer à protéger la confidentialité.

Les accessoires se connectent au serveur d'accès distant à iCloud par HTTP/2, dont la liaison est sécurisée par TLS v1.2 avec AES-128-GCM et SHA-256. L'accessoire garde sa connexion au serveur d'accès distant à iCloud ouverte afin de pouvoir recevoir les messages entrants et envoyer les réponses et les notifications sortantes aux appareils iOS.

Accessoires de télécommande HomeKit

Les accessoires de télécommande HomeKit tiers transmettent des événements d'appareils à interface humain (HID) et des données audio de Siri à une Apple TV associée depuis l'app Domicile. Les événements HID sont envoyés par la session sécurisée entre l'Apple TV et la télécommande. 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. Les pistes audio sont envoyées directement à l'Apple TV par une connexion au réseau local dédiée entre l'Apple TV et la télécommande. La connexion au réseau local dédiée est chiffrée avec une paire de clés par session obtenue par la fonction de dérivation HKDF-SHA-512, qui est négociée au cours de la session HomeKit entre l'Apple TV et la télécommande. 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.

SiriKit

Siri utilise le mécanisme d'extension d'iOS pour communiquer avec les apps tierces. Bien que Siri ait accès aux contacts iOS et à l'emplacement actuel de l'appareil, Siri vérifie l'autorisation d'accès aux données protégées de l'utilisateur iOS par l'app qui contient l'extension avant de fournir ces informations. Siri transmet à l'extension uniquement le segment de texte pertinent provenant de la requête originale de l'utilisateur. Par exemple, si l'app n'a pas accès aux contacts iOS, Siri ne pourra pas interpréter les demandes d'utilisateur comme « Payer ma mère dix dollars avec PaymentApp ». Dans ce cas, l'app de l'extension ne verra que le mot « mère » à travers le fragment brut de l'énoncé transmis. Cependant, si l'app a accès aux contacts iOS, elle recevra les coordonnées iOS de la mère de l'utilisateur. Si un contact est mentionné dans le corps d'un message, par exemple, « Dis à ma mère sur l'app Messages que mon frère est génial », Siri ne résoudra pas « mon frère », quelles que soient les modalités de l'app. Le contenu présenté par l'app peut être envoyé au serveur afin de permettre à Siri de comprendre les instructions de l'utilisateur relatives à l'app.

Dans le cas d'une demande de l'utilisateur comme « Trouve-moi quelqu'un pour me conduire chez ma mère avec <nom de l'app> » pour laquelle des données de localisation doivent être récupérées dans les contacts, Siri fournit ces données à l'extension de l'app uniquement pour cette demande, peu importe l'emplacement ou l'accès aux contacts de l'app.

Lors de l'exécution, Siri permet à l'app sur laquelle SiriKit est activé de fournir un ensemble de mots personnalisés propre à l'instance de l'application. Ces mots personnalisés sont liés à l'identifiant aléatoire décrit dans la section « Siri » du présent document et ont la même durée de vie.

HealthKit

HealthKit stocke et recueille les données provenant des apps de santé et de forme physique avec la permission de l'utilisateur. HealthKit fonctionne aussi directement avec les appareils de santé et de forme physique, comme les moniteurs de fréquence cardiaque compatibles avec Bluetooth Low Energy (BLE) et le coprocesseur de mouvement intégré dans de nombreux appareils iOS.

Données de santé

HealthKit permet aux utilisateurs de stocker et de compiler leurs données de santé provenant de sources comme des apps, des appareils et des établissements de soins de santé. 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 dix 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.

HealthKit agrège 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 de santé principales, puis supprimés une fois la fusion terminée.

Les données de santé peuvent être stockées sur iCloud. Le chiffrement de bout en bout des données de santés requiert iOS 12 ou une version ultérieure ainsi que l'authentification à deux facteurs. Sinon, vos données sont toujours 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), vos données de santé passent au chiffrement de bout en bout.

Si vous effectuez la sauvegarde de votre appareil avec iTunes, vos données de santé sont stockées uniquement quand 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 du 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 v1.2. Après le téléchargement, les dossiers médicaux sont stockés de façon sécurisée avec les autres données de l'app Santé.

Intégrité des données

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 de confiance. Le format utilisé pour la signature numérique est la syntaxe de message cryptographique (CMS, Cryptographic Message Syntax) spécifiée dans le RFC 5652 de l'IETF.

Accès par des apps de tiers

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 de santé pour afficher des publicités. Elles doivent également fournir aux utilisateurs une politique de confidentialité indiquant en détail comment elles utilisent les données de santé.

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

Si des apps sont autorisées à écrire des données, elles peuvent également lire celles-ci. Si elles sont autorisées à lire des données, elles 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 de santé. 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 évite que les apps interfèrent avec l'état de santé de l'utilisateur en s'adaptant aux types de données qui l'intéressent.

Fiche médicale

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 de santé.

Les informations de la fiche médicale peuvent être consultées en touchant le bouton Urgence sur l'écran de verrouillage. 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 enregistrées dans la sauvegarde iCloud et elles ne sont pas synchronisées entre les appareils à l'aide de CloudKit.

ReplayKit

ReplayKit est un cadre d'application qui permet aux développeurs d'ajouter aux apps des capacités 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 des vidéos

L'enregistrement d'une vidéo intègre 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 elle sera 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 d'app dans le démon *replayd* de ReplayKit. Ainsi, le contenu enregistré n'est jamais accessible au processus de l'application.
- **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 empêche l'utilisation des enregistrements par des tiers sans le consentement de l'utilisateur.
- **Aperçu et partage de 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

- **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 point de terminaison 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 garantit que les apps hôtes n'ont aucun privilège pour les contenus vidéo et audio diffusés; seules les extensions de diffusion ReplayKit et de tiers y ont accès.
- **Sélecteur de diffusion :** pour sélectionner le service de diffusion à utiliser, ReplayKit fournit un contrôleur (semblable à UIActivityViewController) que le développeur peut présenter dans son app. Le contrôleur est mis en œuvre à l'aide du SPI UIRemoteViewController et réside sous forme d'extension dans le cadre d'application de ReplayKit. Il se trouve en dehors du processus de l'app hôte.
- **Sélecteur de diffusion du système :** cette fonction permet à l'utilisateur de lancer la diffusion du système directement depuis l'app à l'aide de la même interface utilisateur définie par le système, qui est accessible depuis le centre de contrôle. L'interface utilisateur est mise en œuvre à l'aide du SPI UIRemoteViewController et réside sous forme d'extension dans le cadre d'application de ReplayKit. Il se trouve en dehors du processus de l'app hôte.
- **Extension de téléchargement :** l'extension de téléchargement que les services de diffusion de tiers mettent en œuvre pour traiter le contenu vidéo et audio pendant la diffusion peut choisir de recevoir le contenu de deux façons :
  - petits clips MP4 codés;
  - tampons d'échantillons bruts non codés.
    - **Traitement des clips MP4 :** lorsque ce mode de traitement est appliqué, les petits clips MP4 codés sont générés par *replayd* et stockés dans un emplacement privé qui n'est accessible qu'aux sous-systèmes de ReplayKit. Une fois un plan vidéo généré, *replayd* passe l'emplacement de celui-ci à l'extension de téléchargement de tiers à travers le SPI de requête NSExtension (s'appuyant sur XPC). *replayd* génère également un jeton à usage unique associé à un environnement cloisonné qui est aussi communiqué à l'extension de téléchargement et qui accorde à l'extension l'accès au vidéoclip pendant la demande d'extension.
    - **Traitement des tampons d'échantillons :** lorsque ce mode de traitement est appliqué, les données vidéo et audio sont sérialisées et transmises en temps réel à l'extension tierce de téléchargement au moyen d'une connexion XPC directe. Les données vidéo sont codées en extrayant l'objet IOSurface du tampon échantillon vidéo, en les codant de façon sécuritaire comme objet XPC, en les envoyant à l'extension tierce au moyen de XPC et en les décodant de façon sécuritaire dans un objet IOSurface.

Notes sécurisées

L'app Notes comprend une fonctionnalité de notes sécurisées permettant aux utilisateurs de protéger le contenu de notes précises. Les notes sécurisées sont chiffrées à l'aide d'une phrase secrète fournie par l'utilisateur et requise pour afficher les notes sous iOS et macOS ainsi que sur le site web iCloud.

Lorsqu'un utilisateur sécurise une note, une clé sur 16 octets est calculée d'après la phrase secrète de l'utilisateur grâce aux algorithmes PBKDF2 et SHA256. Le contenu de la note est chiffré par le biais de l'algorithme AES-GCM. Les nouvelles fiches sont créées dans Core Data et CloudKit pour stocker la note, le mot-clé et le vecteur d'initialisation chiffrés, puis les fiches de note d'origine sont supprimées; les données chiffrées ne sont pas écrites sur place. Les pièces jointes sont également chiffrées de cette façon. Parmi les pièces jointes prises en charge, on retrouve les images, les tracés, les tableaux, les plans et les sites web. Les notes contenant d'autres types de pièces jointes ne peuvent pas être chiffrées; celles non prises en charge ne peuvent en outre pas être ajoutées aux notes sécurisées.

Lorsqu'un utilisateur saisit correctement la phrase secrète, que ce soit pour afficher ou pour créer une note sécurisée, Notes ouvre une session sécurisée. Tant que l'app est ouverte, l'utilisateur n'a pas à saisir la phrase secrète ni à utiliser Touch ID ou Face ID pour afficher ou sécuriser d'autres notes. Cependant, si certaines possèdent une phrase secrète différente, la session sécurisée ne s'applique qu'aux notes protégées à l'aide de la phrase secrète active. La session sécurisée se ferme lorsque :

- l'utilisateur touche le bouton Verrouiller dans Notes;
- l'app Notes se trouve en arrière-plan pendant plus de trois minutes;
- l'appareil se verrouille.

Les utilisateurs qui oublient leur phrase secrète peuvent néanmoins afficher leurs notes sécurisées ou sécuriser d'autres notes s'ils activent Touch ID ou Face ID sur leurs appareils. En outre, Notes affiche un indice fourni par l'utilisateur après trois tentatives infructueuses de saisie de la phrase secrète. L'utilisateur doit connaître la phrase secrète en vigueur afin de pouvoir la modifier.

Les utilisateurs peuvent réinitialiser la phrase secrète s'ils ont oublié la phrase active. Cette fonctionnalité permet aux utilisateurs de créer de nouvelles notes sécurisées à l'aide d'une nouvelle phrase secrète, mais celle-ci ne leur permet pas de consulter les notes précédemment sécurisées. Il est toutefois possible d'afficher les notes précédemment sécurisées si l'utilisateur se souvient de l'ancienne phrase secrète. La réinitialisation de la phrase secrète nécessite la phrase secrète du compte iCloud de l'utilisateur.

Notes partagées

Les notes peuvent être partagées avec d'autres utilisateurs. Les notes partagées ne sont pas chiffrées de bout en bout. Apple utilise le type de données chiffrées CloudKit pour tout texte ou toute pièce jointe que l'utilisateur ajoute à une note. Les ressources sont toujours chiffrées avec une clé chiffrée dans CKRecord. Les métadonnées, comme les dates de création et de modification, ne sont pas chiffrées. CloudKit gère le processus utilisé par les participants qui chiffrent ou déchiffrent les données des autres utilisateurs.

Apple Watch

L'Apple Watch fait appel aux fonctionnalités et aux technologies de sécurité conçues pour iOS afin de protéger les données sur l'appareil ainsi que les communications avec l'iPhone jumelé et internet. Cela inclut les technologies telles que la protection des données et le contrôle de l'accès au trousseau. Le code de l'utilisateur est également combiné à l'UID de l'appareil pour créer les clés de chiffrement.

Le jumelage de l'Apple Watch à l'iPhone est sécurisé à l'aide d'un processus hors bande pour l'échange des clés publiques, puis à l'aide du secret partagé de la liaison BLE. L'Apple Watch affiche un motif animé, capturé par l'appareil photo 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 Bluetooth Low Energy établie et chiffrée à l'aide du protocole de sécurité du niveau le plus élevé disponible dans les spécifications de base Bluetooth, l'Apple Watch et l'iPhone échangent des clés par le biais d'un processus dérivé de l'IDS, comme décrit sous « iMessage » dans la section « Services internet » de ce document. Une fois les clés échangées, la clé de session Bluetooth est effacée, et toutes les communications entre l'Apple Watch et l'iPhone sont chiffrées à l'aide de l'IDS; les liaisons Bluetooth, Wi-Fi et cellulaires chiffrées assurent une seconde couche de chiffrement. L'adresse Bluetooth Low Energy est renouvelée toutes les quinze minutes afin de limiter le risque de compromission du trafic.

Pour les apps devant diffuser des données, le chiffrement est assuré à l'aide des méthodes décrites au paragraphe « FaceTime » de la section « Services internet » du présent document, en faisant appel au service IDS fourni par l'iPhone jumelé ou par une connexion internet directe.

L'Apple Watch utilise le chiffrement matériel du stockage et la protection des fichiers et des éléments de trousseau basée sur des classes, comme décrite dans la section « Chiffrement et protection des données » de ce document. 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.

Lorsque l'Apple Watch ne se trouve pas dans le champ Bluetooth, la connexion Wi-Fi ou cellulaire peut être utilisée à la place. L'Apple Watch se joint automatiquement aux réseaux Wi-Fi auxquels le 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. Ce comportement de connexion automatique peut ensuite être configuré selon le réseau dans la section Wi-Fi de l'app Réglages sur l'Apple Watch. Les réseaux Wi-Fi auxquels aucun des deux appareils ne s'est déjà connecté peuvent être accédés manuellement dans la section Wi-Fi de l'app Réglages sur l'Apple Watch.

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 sera transmis à l'Apple Watch dans un format chiffré à l'aide de l'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.

L'Apple Watch peut être verrouillée manuellement en maintenant enfoncé le bouton latéral. En outre, à moins que la détection du poignet soit désactivée, l'appareil est automatiquement verrouillé peu de temps après son retrait du poignet de l'utilisateur. Quand l'Apple Watch est verrouillée, Apple Pay peut être utilisé uniquement après la saisie du code de la montre. La détection du poignet peut être désactivée à l'aide de l'app Apple Watch sur l'iPhone. Ce réglage peut également être appliqué à l'aide d'une solution de GAM.

L'iPhone jumelé peut aussi déverrouiller l'Apple Watch, à condition que celle-ci soit portée. Ce déverrouillage s'effectue après l'établissement d'une connexion authentifiée par les clés définies lors du jumelage. L'iPhone envoie la clé et l'Apple Watch l'utilise pour déverrouiller ses clés de protection des données. Le code de l'Apple Watch n'est ni connu de l'iPhone ni transmis. Cette fonctionnalité peut être désactivée à l'aide de l'app Apple Watch sur l'iPhone.

L'Apple Watch ne peut être jumelée qu'avec un iPhone à la fois. L'iPhone communique des instructions pour effacer l'ensemble du contenu et des données de l'Apple Watch lorsque cette dernière est déjumelée.

L'Apple Watch peut être configurée pour une mise à jour du logiciel système la nuit même. Pour en savoir plus sur le stockage des mots de l'Apple Watch aux fins d'utilisation pendant la mise à jour, consultez la section « Conteneurs de clés » du présent document.

L'activation de la fonctionnalité Localiser mon iPhone sur l'iPhone jumelé permet également l'utilisation du verrouillage d'activation sur l'Apple Watch. Le verrouillage d'activation complique l'usage ou la revente d'une Apple Watch en cas de perte ou de vol. Le verrouillage d'activation oblige l'utilisateur à saisir son identifiant et son mot de passe Apple pour déjumeler, effacer ou réactiver une Apple Watch.

Sécurité du réseau

En plus des dispositifs intégrés mis en place par Apple pour protéger les données stockées sur les appareils iOS, il existe de nombreuses mesures de sécurité réseau que les entreprises peuvent adopter pour sécuriser les informations lors de leur transfert vers un appareil iOS ou à partir de celui-ci.

Les utilisateurs mobiles doivent pouvoir accéder aux réseaux d'entreprise partout dans le monde; il est donc important de s'assurer qu'ils y sont autorisés et que leurs données sont protégées lors des transmissions. iOS utilise des protocoles de mise en réseau standard pour établir des communications authentifiées, autorisées et chiffrées, et permet aux développeurs d'y accéder. Pour atteindre ces objectifs de sécurité, iOS intègre des technologies éprouvées et les normes les plus récentes en matière de connexions aux réseaux de données Wi-Fi et cellulaires.

Sur les autres plateformes, des logiciels coupe-feu sont nécessaires pour protéger les ports de communication ouverts de toute intrusion. Comme iOS réduit la surface d'attaque en limitant les ports d'écoute et en supprimant les utilitaires de réseau inutiles, comme Telnet, les shells ou un serveur web, aucun logiciel coupe-feu supplémentaire n'est nécessaire sur les appareils iOS.

TLS

iOS prend en charge les protocoles TLS (TLS v1.0, TLS v1.1, TLS v1.2, TLS v1.3) et DTLS de sécurité de la couche transport. Il prend en charge les chiffrements AES-128 et AES-256, et préfère les suites de chiffrement offrant une confidentialité persistante impeccable. Safari, Calendrier, Mail et d'autres apps internet utilisent automatiquement ce protocole pour établir un canal de communication chiffré entre l'appareil et les services réseau. Les API de haut niveau (comme CFNetwork) permettent aux développeurs d'adopter facilement le protocole TLS dans leurs apps, tandis que les API de bas niveau (Network.framework) apportent un contrôle fin. L'API CFNetwork n'autorise pas SSL 3. Les apps qui exploitent WebKit (comme Safari) se voient interdire d'établir une connexion SSL 3.

Dans iOS 11 ou version ultérieure et macOS High Sierra ou version ultérieure, les certificats SHA-1 ne sont plus autorisés pour les connexions TLS à moins d'être autorisés par l'utilisateur. Les certificats avec des clés RSA de moins de 2 048 bits sont également rejetés. La suite de chiffrement symétrique RC4 n'est plus prise en charge par iOS 10 et macOS Sierra. Par défaut, les suites de chiffrement RC4 ne sont pas activées sur les clients ou les serveurs TLS mis en œuvre à l'aide des API SecureTransport, donc les clients ou les serveurs TLS ne peuvent pas se connecter lorsque RC4 est la seule suite de chiffrement disponible. Pour assurer un niveau de sécurité plus élevé, les services ou les apps qui requièrent RC4 doivent être mis à niveau afin d'utiliser des suites de chiffrement modernes et sécurisées. Dans iOS 12.1, les certificats émis après le 15 octobre 2018 à partir d'un certificat racine autorisé par le système doivent être inscrits dans un historique autorisé de transparence

de certificat, et ce, pour autoriser leur utilisation dans le cadre de connexions TLS. Dans 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.

Sécurité du transport des apps

La sécurité du transport des apps impose des critères de connexion par défaut de sorte que les apps doivent se conformer aux « bonnes pratiques » en matière de connexions sécurisées lors de l'utilisation des API NSURLConnection, CFURL ou NSURLSession. Par défaut, la sécurité du transport des apps oblige la sélection du chiffrement à n'inclure que les suites qui offrent la confidentialité persistante, notamment ECDHE_ECDSA_AES et ECDHE_RSA_AES en mode GCM ou CBC. Les apps peuvent désactiver l'exigence de confidentialité persistante par domaine, auquel cas RSA_AES est ajouté à l'ensemble de chiffrements disponibles.

Les serveurs doivent prendre en charge TLS v1.2 et la confidentialité persistante, et les certificats doivent être valides et signés par l'algorithme SHA-256 ou une fonction plus évoluée avec une clé RSA sur 2 048 bits ou une clé elliptique de 256 bits minimum.

Les connexions réseau ne satisfaisant pas à ces critères échouent, à moins que l'app outrepasse la sécurité du transport des apps. Les certificats non valides entraînent toujours un échec sec et n'obtiennent aucune connexion. La sécurité du transport des apps est automatiquement appliquée aux applications compilées pour iOS 9 ou version ultérieure.

VPN

Les services réseau sécurisés comme les réseaux privés virtuels ne nécessitent généralement qu'une configuration minime pour fonctionner avec les appareils iOS. Ceux-ci sont compatibles avec les serveurs VPN prenant en charge les protocoles et méthodes d'authentification ci-dessous :

- IKEv2/IPSec avec authentification utilisateur par secret partagé, certificats RSA, certificats **ECDSA**, protocole EAP-MSCHAPv2 ou protocole EAP-TLS;
- SSL-VPN à l'aide de l'app client appropriée qui provient de l'App Store;
- IPSec Cisco avec authentification utilisateur par mot de passe et authentification machine par secret partagé et certificats;
- L2TP/IPSec avec authentification utilisateur par mot de passe MS-CHAPV2 et authentification machine par secret partagé.

iOS prend en charge les fonctionnalités suivantes :

- **VPN à la demande** pour les réseaux qui utilisent une authentification par certificat. Les services informatiques indiquent les domaines qui nécessitent une connexion VPN à l'aide d'un profil de configuration VPN.
- **VPN par app** pour définir beaucoup plus finement quand une connexion VPN doit être établie. La solution de GAM peut spécifier une connexion pour chaque app gérée ou des domaines précis dans Safari. Ce processus permet de garantir que les données confidentielles sont toujours transmises vers le réseau de l'entreprise ou à partir de celui-ci, mais pas les données personnelles d'un utilisateur.

- **VPN permanent**, qui peut être configuré pour les appareils gérés au moyen de la solution de gestion des appareils mobiles (GAM) et supervisés à l'aide d'Apple Configurator 2, d'Apple School Manager ou d'Apple Business Manager. Cela évite aux utilisateurs d'avoir à activer le VPN pour être protégés lorsqu'ils se connectent à des réseaux cellulaires et Wi-Fi. Le VPN permanent offre à une entreprise un contrôle complet sur le trafic des appareils en tunnellisant tout le trafic IP jusqu'à elle. Le protocole de tunnellisation par défaut, IKEv2, sécurise les transmissions 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.

Wi-Fi

iOS prend en charge les protocoles Wi-Fi standard, y compris WPA2 Enterprise, pour offrir un accès authentifié aux réseaux d'entreprise sans fil. WPA2 Enterprise utilise un chiffrement AES 128 bits, qui garantit aux utilisateurs une protection maximale de leurs données lors de l'envoi et de la réception au moyen d'une connexion réseau Wi-Fi. Grâce à la prise en charge de la norme 802.1X, les appareils iOS peuvent être intégrés dans un très grand nombre d'environnements d'authentification RADIUS. Les méthodes d'authentification sans fil 802.1X prises en charge sur l'iPhone et sur l'iPad comprennent EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, PEAPv1 et LEAP.

En plus de la protection des données, iOS étend la protection WPA2 aux cadres de gestion de monodiffusion et de multidiffusion au moyen du service Protected Management Frame mentionné dans 802.11w. La prise en charge de PMF est disponible sur l'iPhone 6 et l'iPad Air 2 ou tout modèle ultérieur.

iOS utilise une adresse Media Access Control (MAC) aléatoire lors des recherches en ligne sans fil tant qu'il n'est pas associé à un réseau Wi-Fi. Ces recherches peuvent être réalisées afin de trouver un réseau Wi-Fi connu et de s'y connecter ou pour 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. Notez que les détections de réseaux qui se produisent lors d'une tentative de connexion à un réseau Wi-Fi connu ne sont pas aléatoires.

iOS utilise également une adresse MAC aléatoire 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 au service de localisation pour des apps utilisant une barrière virtuelle, comme les rappels en fonction du lieu qui déterminent si l'appareil se trouve près d'un lieu précis.

Comme l'adresse MAC d'un appareil change désormais lorsqu'il est déconnecté d'un réseau Wi-Fi, elle ne peut pas être utilisée par des observateurs passifs de trafic Wi-Fi pour suivre en permanence un appareil, même si celui-ci est connecté à un réseau cellulaire. Apple a informé les fabricants de cartes Wi-Fi que les recherches en arrière-plan utilisent une adresse MAC aléatoire et que ni Apple ni les fabricants ne peuvent prédire ces adresses MAC aléatoires. La distribution aléatoire des adresses MAC Wi-Fi n'est pas disponible sur l'iPhone 4s ou antérieur.

Sur l'iPhone 6s et les modèles ultérieurs, la propriété masquée d'un réseau Wi-Fi connu est mise à jour automatiquement. Si l'identificateur SSID (Service Set Identifier) d'un réseau Wi-Fi est diffusé, l'appareil iOS n'enverra pas de sonde comprenant l'identificateur SSID dans la demande. Cette façon de faire empêche l'appareil de diffuser le nom des réseaux non masqués.

Pour protéger l'appareil contre les vulnérabilités du programme interne du processeur réseau, les interfaces réseau, y compris le Wi-Fi et la bande de base, ont un accès limité à la mémoire du processeur d'application. Lorsque le protocole USB ou SDIO est utilisé avec le processeur réseau, ce dernier ne peut pas exécuter de transactions d'accès direct à la 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 IOMMU sur chaque bus PCIe limite l'accès DMA du processeur réseau aux pages de la mémoire contenant ses paquets réseau ou ses structures de contrôle.

Bluetooth

La prise en charge de Bluetooth dans iOS a été conçue pour offrir une fonctionnalité utile sans étendre inutilement l'accès aux données privées. Les appareils iOS prennent en charge les connexions avec mode de chiffrement 3, mode de sécurité 4 et niveau de service 1. iOS prend en charge les profils Bluetooth suivants :

- mains libres (HFP);
- accès à l'annuaire (PBAP);
- accès aux messages (MAP);
- distribution audio avancée (A2DP);
- télécommande audio/vidéo (AVRCP);
- réseau personnel (PAN);
- appareil à interface humaine (HID).

La prise en charge de ces profils dépend de l'appareil.

Pour obtenir plus d'informations, rendez-vous sur :
https://support.apple.com/HT204387

Authentification unique

iOS prend en charge l'authentification aux réseaux d'entreprise par authentification unique (SSO). L'authentification par signature unique fonctionne avec les réseaux utilisant le protocole d'authentification Kerberos pour authentifier les utilisateurs auprès des services auxquels ils sont autorisés à accéder. L'authentification par signature unique peut être utilisée pour de nombreuses activités réseau, des sessions Safari sécurisées aux apps de tiers. L'authentification par certificat (PKINIT) est également prise en charge.

L'authentification par signature unique iOS fait appel à des jetons SPNEGO et au protocole HTTP Negotiate pour fonctionner avec les passerelles d'authentification basées sur Kerberos et les systèmes d'authentification intégrée Windows prenant en charge les tickets Kerberos. La prise en charge de l'authentification par signature unique repose sur le projet Heimdal en code source libre.

Les types de chiffrement suivants sont pris en charge :

- AES-128-CTS-HMAC-SHA1-96;
- AES-256-CTS-HMAC-SHA1-96;
- DES3-CBC-SHA1;
- ARCFOUR-HMAC-MD5.

Safari prend en charge l'authentification par signature unique, et les applications de tiers qui utilisent les API de mise en réseau standard d'iOS peuvent également être configurées pour l'utiliser. Pour configurer l'authentification par signature unique, iOS prend en charge une entité de profil de configuration permettant aux solutions de GAM de transmettre les réglages nécessaires. Cela comprend la définition du nom principal de l'utilisateur (c'est-à-dire, le compte utilisateur Active Directory) et des réglages du domaine Kerberos, ainsi que la configuration des apps ou des URL Safari autorisées à utiliser l'authentification par signature unique.

Continuité

Continuité utilise des technologies comme iCloud, Bluetooth et Wi-Fi pour permettre aux utilisateurs de poursuivre sur un deuxième appareil une activité entamée sur un premier, d'effectuer et de recevoir des appels téléphoniques, d'envoyer et de recevoir des messages texte et de partager une connexion internet mobile.

Handoff

Avec Handoff, lorsque le Mac et les appareils iOS de l'utilisateur sont à proximité les uns des autres, l'utilisateur peut poursuivre son activité d'un appareil à l'autre instantanément.

Lorsqu'un utilisateur se connecte à iCloud sur un deuxième appareil compatible Handoff, les deux appareils établissent un jumelage hors bande Bluetooth Low Energy 4.2 au moyen du service de notification Push d'Apple (APN). Les messages individuels sont chiffrés de la même manière qu'avec iMessage. Une fois les appareils jumelés, chacun génère une clé symétrique AES 256 bits stockée dans le trousseau de chacun d'eux. Cette clé peut chiffrer et authentifier les notifications Bluetooth Low Energy qui communiquent l'activité actuelle de l'appareil aux autres appareils jumelés via iCloud à l'aide d'un algorithme AES-256 en mode GCM, avec des mesures de protection contre la réexécution.

La première fois qu'un appareil reçoit une notification provenant d'une nouvelle clé, il établit une connexion Bluetooth Low Energy à l'appareil émetteur et exécute un échange de clés de chiffrement de notification. Cette connexion est sécurisée par chiffrement Bluetooth Low Energy 4.2 standard ainsi que par un chiffrement des messages individuels (comme dans iMessage). Dans certains cas, ces messages sont transférés via le service APN plutôt que par Bluetooth Low Energy. Le contenu de l'activité est protégé et transféré de la même manière qu'un message iMessage.

Handoff entre sites web et apps natives

Handoff permet à une app iOS native de reprendre des pages web appartenant à des domaines contrôlés de manière légitime par le développeur de l'app. Il autorise également la reprise dans un navigateur web de l'activité de l'utilisateur de l'app native.

Pour 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 biais du mécanisme utilisé pour les accréditations web partagées. Pour en savoir plus à ce sujet, reportez-vous à la sous-section « Accès des apps aux mots de passe enregistrés » de la section « Gestion des mots de passe d'utilisateur » du présent document. 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, comme décrit précédemment.

Sur l'appareil destinataire, 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 destinataire 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 poste-à-poste 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 (voir sections précédentes). Toutefois, après la réception du contenu initial via Bluetooth Low Energy, l'appareil destinataire ouvre une nouvelle connexion via Wi-Fi. Cette connexion est chiffrée (TLS), ce qui implique l'échange de leurs certificats d'identité iCloud. L'identité des certificats est comparée à l'identité de l'utilisateur. Le reste des données de contenu 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 est 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 (comme établi par leur connexion iCloud).

Déverrouillage automatique

Les Mac qui prennent en charge le déverrouillage automatique utilisent Bluetooth Low Energy et le Wi-Fi poste-à-poste pour permettre à l'Apple Watch de l'utilisateur de les déverrouiller de façon sécuritaire. Le Mac compatible et l'Apple Watch associés à un compte iCloud doivent utiliser l'autorisation à deux facteurs.

Lors de l'activation d'une Apple Watch pour déverrouiller un Mac, une liaison sécurisée faisant appel aux identités de déverrouillage automatique est établie. Le Mac crée un secret de déverrouillage unique aléatoire et le transmet à l'Apple Watch au moyen du lien. Le secret est stocké sur l'Apple Watch et n'est accessible que si l'Apple Watch est déverrouillée (voir « Classes de protection des données » dans la section « Chiffrement et protection des données »). Le nouveau secret ne peut pas être identique au mot de passe de l'utilisateur.

Pendant l'opération de déverrouillage, le Mac utilise Bluetooth Low Energy pour établir une connexion avec l'Apple Watch. Un lien sécurisé est établi entre les deux appareils qui utilisent les clés partagées utilisées lors de la première activation. Le Mac et l'Apple Watch utilisent ensuite une connexion Wi-Fi poste-à-poste et une clé sécurisée provenant du lien sécurisé pour déterminer la distance entre les deux appareils. Si les appareils sont à portée l'un de l'autre, le lien sécurisé est utilisé pour transférer le secret prépartagé pour déverrouiller le Mac. Après un déverrouillage réussi, le Mac remplace le secret de déverrouillage actuel par le nouveau secret de déverrouillage unique et transmet le nouveau secret de déverrouillage à l'Apple Watch par le lien.

Relais des appels cellulaires de l'iPhone

Si le Mac, l'iPad ou l'iPod touch d'un utilisateur se trouve sur le même réseau Wi-Fi que l'iPhone de l'utilisateur en question, ce dernier peut effectuer et recevoir des appels téléphoniques à l'aide de la connexion cellulaire de son iPhone. Cette configuration requiert que les appareils soient 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 APN**, chaque notification utilisant le même chiffrement de bout en bout qu'iMessage. Les appareils qui se trouvent sur le même réseau affichent alors l'interface utilisateur de notification d'appel entrant. Lors de la prise de l'appel, le son est correctement transmis à partir de l'iPhone de l'utilisateur par l'entremise d'une connexion poste-à-poste sécurisée entre les deux appareils.

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 Low Energy. 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 l'intermédiaire du service APN, et le son est diffusé de la même façon par la liaison poste-à-poste sécurisée entre les appareils.

Il est possible de désactiver le relais d'appels téléphoniques sur un appareil en désactivant l'option « Appels cellulaires sur iPhone » dans les réglages FaceTime.

Transfert des messages texte de l'iPhone

Le transfert des messages texte envoie automatiquement les SMS reçus sur iPhone à l'iPad, à l'iPod touch ou au Mac enregistré d'un utilisateur. Chaque appareil doit être connecté au service iMessage avec le même identifiant Apple. Lorsque le transfert des 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 reliés, l'iPhone chiffre et transfère les SMS entrants vers chaque appareil en faisant appel aux méthodes décrites sous « iMessage » dans la présente section du document. Les réponses sont renvoyées à l'iPhone à l'aide des 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 des messages texte peut être activé ou désactivé dans les réglages de Messages.

Partage de connexion instantané

Les appareils iOS prenant en charge le partage de connexion instantané utilisent Bluetooth Low Energy pour détecter, et communiquer avec, les appareils connectés au même compte iCloud. Les Mac compatibles, sous OS X Yosemite ou version ultérieure, utilisent la même technologie pour détecter, et communiquer avec, les appareils iOS prenant en charge Instant Hotspot.

Lorsqu'un utilisateur accède aux réglages Wi-Fi de l'appareil iOS, ce dernier émet une annonce Bluetooth Low Energy contenant un identifiant reconnu par tous les autres appareils connectés au même compte iCloud. L'identifiant est généré à partir d'un identifiant DSID (Destination Signaling Identifier) 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.

Lorsqu'un utilisateur choisit un appareil disponible pour le partage de connexion, une requête d'activation du partage de connexion est envoyée à cet appareil. La requête est envoyée via une liaison chiffrée au moyen d'un algorithme standard Bluetooth Low Energy et chiffrée à l'aide d'une méthode de chiffrement similaire à celle d'iMessage. L'appareil répond ensuite via la même liaison Bluetooth Low Energy, en utilisant la même méthode de chiffrement par message avec les informations du partage de connexion.

Sécurité AirDrop

Les appareils iOS qui prennent en charge AirDrop utilisent Bluetooth faible énergie (BLE, Bluetooth Low Energy) et une technologie Wi-Fi poste-à-poste créée par Apple pour envoyer des fichiers et des données aux appareils se trouvant à proximité, notamment les Mac compatibles sous OS X 10.11 ou version ultérieure. Les appareils communiquent directement entre eux par Wi-Fi sans utiliser de connexion internet ni de point d'accès Wi-Fi.

Lorsqu'un utilisateur se connecte au service iCloud, une identité RSA à 2 048 bits est stockée sur l'appareil. Ensuite, quand il active AirDrop, un hachage d'identité AirDrop court est créé à partir des adresses électroniques 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 Bluetooth Low Energy qui comprend le hachage d'identité AirDrop court de l'utilisateur. Les autres appareils à proximité qui sont actifs et sur lesquels AirDrop est activé détectent le signal et répondent par l'entremise du Wi-Fi poste-à-poste. Ainsi, l'appareil expéditeur peut découvrir l'identité de tout appareil qui répond.

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. En mode Contacts, 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 poste-à-poste avec ses informations d'identification. L'appareil expéditeur initie ensuite une connexion AirDrop par l'entremise du Wi-Fi poste-à-poste, et à l'aide de cette connexion, il envoie 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 le prénom et la photo du destinataire sont disponibles dans Contacts, ils s'affichent dans la feuille de partage AirDrop de l'expéditeur.

Lors de l'utilisation d'AirDrop, l'expéditeur sélectionne les personnes avec lesquelles il veut partager des données. 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 vérifiée auprès de l'app Contacts de chaque utilisateur. Le destinataire est alors invité à accepter le transfert entrant en provenance de la personne ou de l'appareil identifiés. Si plusieurs destinataires ont été sélectionnés, ce processus est répété pour chaque destination.

En mode Tout le monde, le même processus est utilisé, mais si aucune correspondance n'est trouvée dans Contacts, les appareils récepteurs apparaissent dans la feuille de partage AirDrop avec une silhouette et le nom de l'appareil défini dans Réglages > Général > Informations > Nom.

Les entreprises peuvent restreindre l'usage d'AirDrop pour les apps ou les appareils gérés par une solution de GAM.

Partage de mot de passe Wi-Fi

Les appareils iOS qui prennent en charge le partage de mot de passe Wi-Fi ont recours à un mécanisme similaire 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 annonce Bluetooth Low Energy 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 Bluetooth Low Energy.

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 similaire à AirDrop. Une fois l'identité confirmée, le cédant envoie au demandeur la clé prépartagée de 64 caractères, qui peut également être utilisée 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 GAM.

Apple Pay

Grâce à Apple Pay, les utilisateurs peuvent se servir des appareils iOS pris en charge, une Apple Watch et un Mac pour effectuer en toute simplicité des paiements de façon sûre et confidentielle dans les magasins, dans les applications et à partir de Safari. Les utilisateurs peuvent également ajouter à Wallet les cartes de transport compatibles avec Apple Pay. Ce système est simple pour les utilisateurs et sécurisé sur les plans matériel et logiciel.

Apple Pay est aussi conçu pour protéger les informations personnelles de l'utilisateur. Il ne collecte aucune information relative aux transactions pouvant être associée à ce dernier. Les opérations de paiement sont réalisées entre l'utilisateur, le vendeur et l'émetteur de la carte.

Composants d'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.

Contrôleur NFC : le contrôleur NFC 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.

Wallet : 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 consulter leurs cartes et potentiellement des informations supplémentaires fournies par l'émetteur de leur carte, comme la politique de confidentialité de celui-ci, les transactions récentes et plus encore dans Wallet. Les utilisateurs peuvent également ajouter des cartes à Apple Pay dans :

- Assistant de configuration et Réglages sur iOS;
- l'app Watch sur l'Apple Watch;
- Wallet et Apple Pay dans Préférences Système sur Mac.

En outre, 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 l'iPhone, l'iPad et l'Apple Watch, le Secure Enclave gère le processus d'authentification et permet l'exécution des opérations de paiement.

Sur l'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 (le cas échéant) 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 crédit, de débit et de transport dans Wallet, et 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.

Comment Apple Pay utilise le Secure Element

Le Secure Element renferme un applet spécifiquement conçu pour gérer Apple Pay. Il comporte également des applets de paiement 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 via le contrôleur de communication en champ proche (NFC) au moyen d'un bus matériel dédié.

Comment Apple Pay utilise le contrôleur NFC

En tant que passerelle vers le Secure Element, le contrôleur NFC s'assure que toutes les opérations de paiement sans contact sont 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 NFC.

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 NFC par le contrôleur. Les détails de l'autorisation de paiement pour les transactions de paiement sans contact sont donc transmis uniquement au champ NFC 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.

Approvisionnement des cartes de crédit, de débit et prépayées

Lorsqu'un utilisateur ajoute une carte de crédit, de débit ou prépayée (ou la carte d'un magasin) à 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 service autorisé de l'émetteur de la carte. À l'aide de ces informations, l'émetteur de carte décide d'approuver ou non l'ajout de la carte à Wallet.

Apple Pay utilise trois appels côté serveur pour communiquer avec l'émetteur de carte ou le réseau dans le cadre du processus de transfert d'une carte : *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 Wallet. Ces sessions client-serveur sont chiffrées à l'aide du protocole TLS v1.2.

Les numéros de carte complets ne sont stockés ni sur l'appareil ni sur les serveurs d'Apple. À la place, un numéro de compte d'appareil est créé, chiffré puis stocké dans le Secure Element. Ce numéro unique est chiffré de sorte qu'Apple ne puisse pas y accéder. Le numéro de compte d'appareil étant unique et différent des numéros de carte de paiement habituels, 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 d'appareil conservé dans le Secure Element est isolé d'iOS et de watchOS, et n'est jamais stocké sur les serveurs Apple ni sauvegardé dans iCloud.

Les cartes utilisées avec l'Apple Watch sont transférées pour Apple Pay à l'aide de l'app Watch sur l'iPhone ou dans l'app pour iPhone des émetteurs de cartes. L'ajout d'une carte à l'Apple Watch nécessite que celle-ci se trouve à portée Bluetooth. Les cartes sont spécifiquement enregistrées pour une utilisation avec l'Apple Watch et possèdent leur propre numéro de compte d'appareil, stocké dans le Secure Element sur l'Apple Watch.

Lorsque des cartes prépayées, de crédit ou de débit (y compris les cartes de magasin) sont ajoutées, elles s'affichent dans une liste de cartes pendant l'assistant de configuration sur les appareils connectés au même compte iCloud. Ces cartes demeurent dans cette liste tant qu'elles sont actives sur au moins un appareil. Les cartes sont supprimées de cette liste lorsqu'elles sont supprimées de tous les appareils depuis sept jours. Cette fonctionnalité requiert que l'authentification à deux facteurs soit activée sur le compte iCloud respectif.

Ajout manuel d'une carte bancaire à Apple Pay

Lors de l'ajout manuel d'une carte, le nom, le numéro de carte, la date d'expiration et le code CVV sont utilisés pour faciliter le processus de transfert. Les utilisateurs peuvent saisir 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 capture les informations de la carte, Apple tente de remplir les champs du nom, 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 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 concerné 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 de vos comptes iTunes et App Store (par exemple, si vous effectuez souvent des transactions dans iTunes), des renseignements sur votre appareil (par exemple, le numéro de téléphone, le nom et le modèle de ce dernier, ainsi que ceux de tout appareil iOS complémentaire nécessaire à la configuration d'Apple Pay) et votre 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 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 Wallet représentant la carte bancaire.
- L'appareil commence à associer la carte au Secure Element.

Le fichier de billet 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 du billet qui comprend des informations indiquant par exemple si la personnalisation du Secure Element est terminée, si la carte est actuellement suspendue par l'organisme 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 crédit ou de débit à Apple Pay à partir d'un compte iTunes Store

Pour les cartes de débit ou de crédit 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 bancaire à partir de l'app d'un émetteur de carte

Lorsque l'app est inscrite pour être exploitée avec Apple Pay, les clés sont établies pour l'app 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 la carte, ce qui empêche l'appareil iOS de lire ces informations. Le flux de transfert ressemble à celui des cartes ajoutées manuellement, décrites ci-dessus, hormis que des mots de passe à usage unique sont utilisés au lieu des codes CVV.

Vérification supplémentaire

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 client 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 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 du paiement

Sur les appareils dotés du Secure Enclave, le Secure Element approuvera les paiements uniquement après avoir reçu l'autorisation du Secure Enclave. Sur l'iPhone ou l'iPad, cela suppose que l'utilisateur s'identifie avec Touch ID, Face ID ou le code de l'appareil. Touch ID et Face ID constituent les méthodes par défaut si disponibles, mais il est possible d'utiliser à tout moment la vérification par code. 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. Sur l'Apple Watch, l'appareil doit être déverrouillé à l'aide du code, et un double-clic sur le bouton latéral est nécessaire pour effectuer un paiement.

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 NFC 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 la norme standard AES, et des nonces de chiffrement sont utilisés des deux côtés pour assurer la protection contre les attaques par réinsertion. 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 de manière sécurisée à partir du Secure Enclave en usine jusqu'à un **module de sécurité matériel (HSM)** qui dispose du matériel nécessaire pour ensuite injecter la clé de jumelage dans le Secure Element.

Lorsque l'utilisateur autorise une transaction, le Secure Enclave 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 paiement et est conservée tant qu'Apple Pay est activé. Elle est protégée par le chiffrement et le mécanisme antirecul du Secure Enclave. Elle est transmise de manière sécurisée 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.

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 AR utilisées lors de l'ajout de la carte. Cela permet à iOS d'ordonner au Secure Enclave de rendre des cartes inutilisables en marquant la copie de la valeur AR en sa possession comme invalide lorsque :

- le code est désactivé;
- l'utilisateur se déconnecte d'iCloud;
- l'utilisateur sélectionne Effacer contenu et réglages;
- l'appareil est restauré à partir du mode de récupération.

Avec l'Apple Watch, les cartes sont signalées comme non valides lorsque :

- le code d'Apple Watch est désactivé;
- l'Apple Watch n'est plus jumelée avec l'iPhone.

Avec la clé de jumelage et sa copie de la valeur AR actuelle, le Secure Element vérifie l'autorisation envoyée par le Secure Enclave avant d'activer l'applet de paiement pour effectuer un paiement sans contact. Ce processus est également utilisé pour récupérer des données de paiement chiffrées à partir d'un applet de paiement pour des transactions effectuées dans des apps.

Code de sécurité dynamique propre à la transaction

Les transactions de paiement provenant d'applets de paiement comprennent un cryptogramme de paiement ainsi qu'un numéro de compte d'appareil. Ce cryptogramme, un code à usage unique, est calculé à l'aide d'un compteur de transactions qui augmente à chaque nouvelle transaction et d'une clé mise à disposition dans l'applet de paiement au cours de la personnalisation. Ce code est connu par le réseau de paiement ou 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 nombre aléatoire généré par le terminal en cas de transaction NFC;
- un nonce généré par le serveur Apple Pay en cas de transaction effectuée dans une app.

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

Paiement avec cartes de crédit ou de débit dans les magasins

Lorsque l'iPhone est activé et qu'il détecte un champ NFC, 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 d'appareil et un code de sécurité dynamique propre à la transaction sont utilisés lors du traitement du paiement. Ni Apple ni l'appareil de l'utilisateur n'envoient les numéros complets de carte bancaire 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 avec cartes de crédit ou de débit dans les apps

Apple Pay peut également être utilisé pour effectuer des paiements dans les apps iOS et l'Apple Watch. Lorsque des utilisateurs effectuent des paiements dans des apps à l'aide d'Apple Pay, Apple reçoit des données de transaction chiffrées qu'elle chiffre à nouveau au moyen d'une clé propre à chaque développeur avant de les envoyer à ce dernier ou au vendeur. 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. Les serveurs Apple Pay chiffrent à nouveau ces données au moyen d'une clé propre au vendeur avant de transmettre la transaction 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 bancaires capables d'effectuer des paiements sur les réseaux de paiement acceptés par le vendeur. L'app demande les éléments d'information 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 de présenter la feuille Apple Pay qui demande les informations relatives à l'app ainsi que d'autres informations nécessaires, telles que la carte à utiliser.

L'app reçoit alors les informations relatives à la ville, à la région 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.

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 NFC 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. Elle est ensuite renvoyée à l'appareil qui la 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 à envoyer au Secure Element en vue de leur signature, comme le numéro de commande ou l'identité du client, afin de veiller à ce que la transaction ne puisse pas être détournée vers un autre client. Cette tâche est effectuée par le développeur de l'app, qui peut indiquer les données d'application (applicationData) de la demande de paiement (PKPaymentRequest). Un hachage de cette donnée est inclus dans les données de paiement chiffrées. Le vendeur doit ensuite vérifier que le hachage de ses données d'application correspond à ce qui se trouve dans les données de paiement.

Paiement avec cartes de crédit ou de débit sur le web

Apple Pay peut être utilisé pour effectuer des paiements sur les sites web avec des appareils iOS, une Apple Watch ou un Mac. Les transactions Apple Pay peuvent également être initiées 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. Les serveurs Apple effectuent une validation du nom de domaine et émettent un certificat de client TLS. Les sites web qui prennent en charge Apple Pay doivent fournir leur contenu au moyen de 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 Apple Pay et si une carte de crédit, de débit ou prépayée est activée sur l'appareil. Aucun autre détail n'est partagé. Si l'utilisateur ne veut pas partager ces informations, il peut désactiver les requêtes Apple Pay dans les paramètres de confidentialité de Safari sur iOS et macOS.

Une fois qu'une session de vendeur est validée, toutes les mesures de sécurité et de confidentialité sont les mêmes que lorsqu'un utilisateur effectue un paiement dans une app.

Dans le cas d'une transmission Handoff d'un Mac à l'iPhone ou à l'Apple Watch, Apple Pay utilise le protocole IDS chiffré de bout en bout pour transmettre les informations de paiement 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. Les clés ne sont pas accessibles par Apple. La détection d'appareils requise par Apple Pay pour effectuer une transmission Handoff contient le type, l'identifiant unique et certaines métadonnées des cartes de crédit de l'utilisateur. Le numéro de compte de l'appareil de la carte de l'utilisateur n'est pas partagé et continue d'être stocké de façon sécurisée sur l'iPhone ou l'Apple Watch de l'utilisateur.

Apple transfère également de façon sécurisée les adresses de contact, 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 qu'il appuie deux fois sur le bouton latéral de l'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 Low Energy.

Cartes sans contact

Wallet prend en charge le protocole de service à valeur ajoutée (VAS) pour la transmission des données de cartes reconnues vers les terminaux NFC compatibles. Le protocole VAS peut être mis en œuvre sur les lecteurs sans contact et exploite la technologie NFC pour communiquer avec les appareils Apple pris en charge. Le protocole VAS fonctionne sur une courte distance et peut être utilisé pour présenter séparément des cartes sans contact ou dans le carte d'une transaction Apple Pay.

Lorsque l'appareil est tenu près du terminal NFC, 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 vendeur, il doit autoriser son utilisation à l'aide de Touch ID, de Face ID ou de son code. Les informations sur la carte, un horodatage et une clé ECDH P-256 aléatoire à usage unique sont utilisés conjointement avec la clé publique du vendeur pour calculer une clé de chiffrement pour les données de la carte, lesquelles sont envoyées au terminal.

Les utilisateurs peuvent aussi sélectionner manuellement une carte, puis l'autoriser à l'aide de Touch ID, Face ID ou du code avant de la présenter au terminal NFC du vendeur.

Apple Pay Cash

Avec iOS 11.2 ou version ultérieure et watchOS 4.2 ou version ultérieure, Apple Pay peut être utilisé sur un iPhone, un iPad ou une Apple Watch pour envoyer de l'argent à d'autres utilisateurs, en recevoir de leur part ou leur en demander. Lorsqu'un utilisateur reçoit de l'argent, la somme est créditée sur un compte Apple Pay Cash accessible dans 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.

Pour utiliser les paiements de personne à personne et Apple Pay Cash, un utilisateur doit être connecté à son compte iCloud sur un appareil compatible avec Apple Pay Cash et y avoir configuré l'authentification à deux facteurs.

Lorsque vous configurez Apple Pay Cash, des informations similaires à celles que vous partagez lorsque vous ajoutez une carte de crédit ou de débit pourraient être partagées avec notre banque partenaire, Green Dot Bank, et Apple Payments Inc., une filiale qui appartient à Apple dans sa totalité, créée pour stoker et traiter les informations séparément du reste des données

d'Apple et ainsi protéger vos données confidentielles. Ces informations sont utilisées uniquement à des fins réglementaires, de dépannage et de prévention de la fraude.

Les demandes et les transferts d'argent entre utilisateurs sont initiés à partir de l'app Messages ou par l'intermédiaire de Siri. Lorsqu'un utilisateur tente d'envoyer de l'argent, iMessage affiche la feuille Apple Pay. Le solde Apple Pay Cash est toujours utilisé en premier. Au besoin, des fonds supplémentaires sont débités d'une carte de crédit ou de débit que l'utilisateur a ajoutée à Wallet.

La carte Apple Pay Cash dans 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 Pay 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 Pay Cash à partir d'une carte de débit ou d'une carte prépayée dans Wallet.

Apple Payments Inc. stocke vos données de transaction 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 vous envoyez de l'argent, de qui vous en recevez, ni les endroits où vous effectuez des achats avec votre carte Apple Pay Cash.

Lorsque vous envoyez de l'argent avec Apple Pay, en ajoutez à un compte Apple Pay Cash ou en transférez vers un compte bancaire, un contact est établi avec les serveurs Apple Pay afin d'obtenir un nonce cryptographique similaire à la valeur retournée pour Apple Pay dans les apps. Le nonce, ainsi que les autres données de transaction, est envoyé au Secure Element pour générer une signature de paiement. Lorsque la signature de paiement sort du Secure Element, elle est transmise aux serveurs Apple Pay. L'authentification, 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 initié, et vous êtes avisé de la réussite de la transaction.

Si la transaction concerne une carte de crédit ou de débit pour ajouter de l'argent à Apple Pay Cash, en envoyer à un autre utilisateur ou compléter le solde Apple Pay Cash si ce dernier est insuffisant, une accréditation de paiement chiffrée est également générée et envoyée aux serveurs Apple Pay, une procédure similaire à celle utilisée par Apple Pay dans les apps et sur les sites web.

Si le solde Apple Pay Cash excède un certain montant ou qu'une activité inhabituelle est détectée, l'utilisateur sera 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 de son adresse antérieure), sont transmises de façon sécurisée aux partenaires d'Apple et chiffrées à l'aide de leur clé. Apple n'est pas en mesure de déchiffrer ces données.

Cartes de transport

En Chine et au Japon, les utilisateurs peuvent ajouter les cartes de transport prises en charge dans Wallet, sur les modèles compatibles d'iPhone et d'Apple Watch. On peut faire cet ajout soit en transférant la valeur et le titre de transport d'une carte physique vers sa représentation numérique dans Wallet ou en transférant une nouvelle carte de transport dans Wallet à partir de l'app de l'émetteur de cette carte. Une fois les cartes de transport ajoutées à Wallet, les utilisateurs peuvent utiliser les transports en commun simplement en tenant leur iPhone ou leur Apple Watch près du lecteur. Au Japon, la carte Suica peut également être utilisée 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 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. Par exemple, les cartes MySuica peuvent être liées aux cartes Suica anonymes. 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 Wallet, les utilisateurs sont invités à saisir certains chiffres du numéro de série de la carte. Les utilisateurs peuvent également devoir fournir des renseignements personnels pour prouver qu'ils ont la carte en main. Par exemple, s'il s'agit d'une carte MySuica ou d'une carte contenant un titre de transport, les utilisateurs doivent également saisir leur date de naissance. Lors du transfert des cartes d'un iPhone vers une Apple Watch, les deux appareils doivent être en ligne.

Il est possible de recharger le solde avec des fonds provenant de cartes de crédit ou de cartes prépayées à partir de Wallet ou de l'app de l'émetteur de la carte de transport. La sécurité de la recharge du solde à l'aide d'Apple Pay est décrite dans la section « Paiement avec cartes de crédit ou de débit dans les apps » du présent document.

Le processus de transfert de la carte de transport à partir de l'app de l'émetteur de cette carte est décrit dans la section « Ajout d'une carte bancaire à partir de l'app d'un émetteur de carte » du présent document.

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. Une fois la vérification effectuée, le système peut créer un numéro de compte d'appareil pour le Secure Element et activer la nouvelle carte dans Wallet avec le solde transféré. Au Japon, après son transfert, la carte physique Suica est désactivée.

Au terme de ces méthodes de transfert, le solde de la carte de transport est chiffré et stocké dans un applet désigné dans le Secure Element. L'opérateur 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 de 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 dans les réglages Wallet et Apple Pay en désactivant Transport express.

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 mon iPhone;
- activant le mode Perdu avec Localiser mon iPhone;
- utilisant la commande d'effacement à distance de la gestion des appareils mobiles;
- 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 Wallet;
- supprimant la carte de l'app de l'émetteur.

Les serveurs Apple Pay avisent alors l'opérateur de transport en commun de suspendre ou de désactiver ces cartes. Pour les cartes Suica, si les appareils des utilisateurs sont hors ligne lors de l'effacement, les cartes Suica restent utilisables jusqu'à 0 h 01 (heure du Japon) le jour suivant. Si l'appareil de l'utilisateur est hors ligne, les cartes de transport en Chine continuent d'être utilisables.

Si les utilisateurs suppriment leurs cartes de transport, le solde est récupérable en les rajoutant à un appareil connecté avec le même identifiant Apple.

Cartes étudiantes

Sous iOS 12, les étudiants, les membres des facultés et les employés des campus participants peuvent ajouter leur carte d'identité à Wallet pour accéder à certains endroits et payer partout où leur carte est acceptée.

Un utilisateur ajoute sa carte d'identité à Wallet depuis une app fournie par l'émetteur de la carte ou par l'école participante. Le processus technique est le même que celui décrit dans la section « Ajout d'une carte bancaire à partir de l'app d'un émetteur de carte » du présent document. En outre, les apps émettrices doivent prendre en charge l'authentification à deux facteurs sur les comptes qui protègent l'accès à leurs cartes d'identité. 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 Wallet, le mode Express est activé par défaut. Les cartes étudiantes en mode Express interagissent avec les terminaux compatibles sans l'authentification par Touch ID, Face ID ou code. L'utilisateur peut toucher le bouton Plus sur le devant de la carte d'identité dans Wallet et désactiver la fonctionnalité 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 mon iPhone;
- activant le mode Perdu avec Localiser mon iPhone;
- utilisant la commande d'effacement à distance de la gestion des appareils mobiles;
- 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 Wallet;
- supprimant la carte de l'app de l'émetteur.

Suspension, retrait et suppression de cartes

Les utilisateurs ont la possibilité de suspendre Apple Pay sur leur iPhone, leur iPad et leur Apple Watch en plaçant leur appareil en mode Perdu à l'aide de Localiser mon iPhone. Ils peuvent également retirer et supprimer leurs cartes d'Apple Pay au moyen de la fonctionnalité Localiser mon iPhone, sur iCloud.com ou directement sur leur appareil à l'aide de Wallet. Les cartes enregistrées dans l'Apple Watch peuvent être supprimées à l'aide des réglages iCloud, dans l'app Apple Watch sur l'iPhone ou directement sur la montre. L'émetteur de la carte ou le réseau de paiement concerné suspend ou supprime alors la possibilité d'effectuer des paiements avec les cartes à l'aide d'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 leur carte pour suspendre ou retirer des cartes d'Apple Pay.

Par ailleurs, lorsqu'un utilisateur efface l'intégralité du contenu de son appareil à l'aide de la commande « Effacer contenu et réglages » avec Localiser mon iPhone ou en restaurant son appareil en mode de récupération, iOS demande au Secure Element de marquer toutes les cartes comme supprimées. Cette opération rend immédiatement 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 de paiement avec des cartes précédemment enregistrées. Une fois en ligne, l'appareil essaie de contacter les serveurs Apple Pay pour s'assurer que toutes les cartes présentes dans le Secure Element sont effacées.

Services internet

Création de mots de passe robustes d'identifiant Apple
Les identifiants Apple sont utilisés pour se connecter à différents services comme iCloud, FaceTime et iMessage. Pour aider les utilisateurs à créer des mots de passe complexes, les critères suivants sont imposés :

- au moins huit caractères;
- au moins une lettre;
- au moins une lettre majuscule;
- au moins un chiffre;
- pas plus de trois caractères identiques consécutifs;
- différent du nom du compte.

Apple a créé une série de services fiables destinés à rendre les appareils de ses utilisateurs encore plus pratiques et productifs; ces services comprennent notamment iMessage, FaceTime, les suggestions de Siri, iCloud, la sauvegarde iCloud et le trousseau iCloud.

Ces services internet ont été développés avec les mêmes objectifs de sécurité que ceux mis en avant par iOS dans la plateforme. Ces objectifs incluent la manipulation sécurisée des données, que ce soit au sein des appareils ou lors de leur transfert à travers des réseaux sans fil; la protection des données personnelles des utilisateurs; et la protection contre tout accès malveillant ou non autorisé aux informations et aux services. Chaque service utilise sa propre architecture de sécurité performante sans compromettre la facilité d'utilisation générale du système iOS.

Identifiant Apple

L'identifiant Apple correspond au compte utilisé pour se connecter à des services comme iCloud, iMessage, FaceTime, l'iTunes Store, l'App Store, Apple Books et bien plus encore. Il est essentiel que chaque utilisateur protège son identifiant Apple afin d'éviter tout accès non autorisé à ses comptes. Pour cela, Apple conseille d'utiliser des mots de passe complexes composés d'au moins huit caractères, comprenant à la fois des lettres et des chiffres, n'incluant pas plus de trois caractères identiques consécutifs et différents des mots de passe 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 oblige également les utilisateurs à créer trois questions de sécurité permettant de vérifier l'identité du propriétaire en cas de modification de ses informations de compte ou de réinitialisation d'un mot de passe oublié.

Apple envoie également à ses utilisateurs des messages électroniques et des notifications lorsque des modifications importantes sont apportées à leur compte, par exemple en cas de changement de mot de passe ou de données de facturation, ou encore d'utilisation de l'identifiant Apple pour se connecter à un nouvel appareil. Les utilisateurs sont de plus invités à changer le mot de passe de leur identifiant Apple dès qu'ils remarquent quoi que ce soit d'inhabituel.

En outre, Apple emploie une panoplie étendue de règlements et de procédures conçus pour protéger les comptes utilisateur. Parmi ces dispositions, on retrouve la limitation du nombre de tentatives d'ouverture de session et de réinitialisation du mot de passe, le contrôle actif antifraude pour aider à identifier les attaques dès qu'elles se produisent, ainsi que des passages en revue routiniers des lignes de conduite pour aider Apple à s'adapter à toute nouvelle information susceptible de compromettre la sécurité des clients.

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.

Cette authentification à deux facteurs permet à un utilisateur d'accéder à son compte uniquement sur des appareils de confiance, comme son iPhone, son iPad ou son Mac. Pour ouvrir une première session sur un nouvel appareil, deux informations sont obligatoires : le mot de passe de l'identifiant Apple et un code de vérification à six chiffres automatiquement affiché sur les appareils de confiance de 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 ouvrir une session. Dans la mesure où un mot de passe seul n'est plus suffisant pour accéder au compte d'un utilisateur, l'authentification à deux facteurs est recommandée. Cette technique est directement intégrée à iOS, à macOS, à tvOS, à watchOS et aux systèmes d'authentification employés par les sites web d'Apple.

Pour en savoir plus sur l'authentification à deux facteurs, rendez-vous sur : https://support.apple.com/HT204915

Vérification en deux étapes

Apple propose en outre, depuis 2013, un moyen sécurisé similaire appelé *vérification en deux étapes*. Lorsque cette méthode est activée, l'identité de l'utilisateur doit être vérifiée au moyen d'un code temporaire envoyé à l'un de ses appareils de confiance, avant d'autoriser toute modification des informations de compte liées à son identifiant Apple, avant toute connexion à iCloud, à iMessage, à FaceTime ou au Game Center, ou avant tout achat sur l'iTunes Store, l'App Store ou Apple Books à partir d'un nouvel appareil. Les utilisateurs disposent également d'une clé de récupération de quatorze caractères à conserver en lieu sûr en cas d'oubli de leur mot de passe ou de perte d'accès à leurs appareils de confiance. La plupart des nouveaux utilisateurs seront incités à utiliser l'authentification à deux facteurs, mais il existe encore quelques situations pour lesquelles la validation en deux étapes est recommandée.

Pour en savoir plus sur la vérification d'identifiant Apple en deux étapes, rendez-vous sur : https://support.apple.com/HT204152

Identifiants Apple gérés

Les identifiants Apple gérés fonctionnent comme les identifiants Apple, mais sont détenus et contrôlés par un établissement d'enseignement. L'établissement peut 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.

Certains services Apple sont désactivés pour les identifiants Apple gérés, comme Apple Pay, le trousseau iCloud, HomeKit et Localiser mon iPhone.

Pour en savoir plus sur les identifiants Apple gérés, rendez-vous sur : https://help.apple.com/schoolmanager/#/tes78b477c81

Audit des identifiants Apple gérés

Les identifiants Apple gérés prennent également en charge l'audit, ce qui permet aux établissements de respecter la réglementation en vigueur et les règles de confidentialité. Les comptes administrateur, gestionnaire ou professeur peuvent se voir accorder des privilèges d'audit pour certains identifiants Apple gérés. Les auditeurs sont en mesure de contrôler uniquement les comptes qui dépendent d'eux dans la hiérarchie de l'école. En d'autres termes, les enseignants peuvent surveiller les élèves, les gestionnaires peuvent auditer les enseignants et les élèves, et les administrateurs peuvent effectuer l'audit des gestionnaires, des enseignants et des élèves.

Lorsque des informations d'authentification associées à la réalisation d'un audit sont demandées par le biais d'Apple School Manager, un compte particulier est émis dont l'accès est limité à l'identifiant Apple géré pour lequel l'audit est demandé. L'autorisation d'audit expire au bout de sept jours. Au cours de cette période, l'auditeur peut lire et modifier le contenu de l'utilisateur stocké sur iCloud ou dans les apps qui utilisent CloudKit. Chaque demande d'accès à l'audit est consignée dans Apple School Manager. Les journaux indiquent qui est l'auditeur, l'identifiant Apple géré auquel l'auditeur a demandé accès, l'heure de la demande et si l'audit a été réalisé.

Pour en savoir plus sur l'inspection des identifiants Apple gérés, rendez-vous sur : https://help.apple.com/schoolmanager/#/tesd8fcbdd99

Identifiants Apple gérés et appareils personnels

Les identifiants Apple gérés peuvent également être utilisés avec des appareils iOS ou des ordinateurs Mac personnels. Les élèves ouvrent une session iCloud avec l'identifiant Apple géré émis 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. Lors de l'utilisation d'un identifiant Apple géré sur un appareil personnel, le trousseau iCloud est indisponible et l'établissement peut restreindre d'autres fonctionnalités. Tout document iCloud créé par des élèves lorsque leur session est active est susceptible de faire l'objet d'un audit comme décrit précédemment dans la présente section.

iMessage

Conçu par Apple, iMessage est un service de messagerie pour appareils iOS, Apple Watch et ordinateurs Mac. iMessage prend en charge aussi bien le texte que les pièces jointes, telles que les photos, les contacts et les lieux. Les messages apparaissent sur tous les appareils enregistrés d'un utilisateur, de telle sorte qu'une conversation entamée sur un appareil puisse être poursuivie sur n'importe quel autre appareil. iMessage utilise le service de notification Push d'Apple (Apple Push Notification ou APN) de manière intensive. Apple ne conserve pas le contenu des messages ou 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, ce dernier génère deux paires de clés à utiliser avec le service : une clé RSA 1 280 bits pour le chiffrement et une clé ECDSA 256 bits sur la courbe NIST P-256 pour la signature. Les clés privées des deux paires de clés sont enregistrées dans le trousseau de l'appareil, tandis que les clés publiques sont envoyées

au service d'identité Apple (IDS) où elles sont associées au numéro de téléphone ou à l'adresse électronique de l'utilisateur, ainsi qu'à l'adresse du service APN de l'appareil.

Au fur et à mesure que les utilisateurs activent des appareils supplémentaires à utiliser avec iMessage, leurs clés publiques de chiffrement et de signature, 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 demandera 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.

Dans iOS 12 ou version ultérieure, les messages envoyés à partir de différentes adresses qui sont liées au même identifiant Apple s'affichent comme une seule conversation sur les appareils qui les reçoivent. Cela est permis par un identifiant de compte récupéré auprès de l'IDS avec les clés publiques ainsi que les adresses de service APN pour une adresse courriel ou un numéro de téléphone.

Envoi et réception 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 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 individuellement pour chacun des appareils du destinataire. Les clés de chiffrement RSA publiques des appareils destinataires sont récupérées via le service 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 d'AES en mode CTR. 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 destinataire. 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 à l'aide de la clé de signature privée de l'appareil expéditeur. Les messages résultants (un pour chaque appareil destinataire) 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 le code temporel 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. Si le texte du message est trop long ou qu'une pièce jointe (telle qu'une photo) est incluse, la pièce jointe est chiffrée par AES en mode CTR à l'aide d'une clé 256 bits générée aléatoirement et 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).

Dans le cas d'une conversation de groupe, ce processus est répété pour chaque destinataire et ses appareils.

Du côté destinataire, chaque appareil reçoit sa copie du message par le biais du service APN et, si nécessaire, récupère la pièce jointe sur iCloud. L'adresse électronique de l'expéditeur ou le numéro de téléphone de l'appelant 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 actuellement conservés pendant 30 jours au maximum.

Clavardage d'entreprise

Le clavardage d'entreprise est un service de messagerie qui permet aux utilisateurs de communiquer avec des entreprises au moyen de l'app Messages. Seuls les utilisateurs peuvent entamer la conversation et l'entreprise reçoit un identifiant opaque pour chacun d'eux. L'entreprise ne reçoit ni le numéro de téléphone de l'utilisateur, ni son adresse courriel, ni les informations de son compte iCloud. Lorsque vous clavardez avec Apple, elle reçoit un identifiant de clavardage d'entreprise associé à votre identifiant Apple. Les utilisateurs décident eux-mêmes s'ils veulent communiquer. La suppression d'une conversation de clavardage d'entreprise l'efface de l'app Messages de l'utilisateur et empêche l'entreprise de continuer à lui envoyer des messages.

Chacun des messages envoyés à l'entreprise est chiffré entre l'appareil de l'utilisateur et les serveurs de messagerie d'Apple; ceux-ci déchiffrent ensuite les messages et les relaient à l'entreprise par protocole TLS. De la même façon, les réponses des entreprises sont envoyées par protocole TLS aux serveurs de messagerie d'Apple, qui rechiffrent ensuite le message vers l'appareil de l'utilisateur. Comme pour iMessage, l'envoi des messages est mis en attente sur les appareils hors ligne pendant une période pouvant atteindre 30 jours.

FaceTime

FaceTime est le service d'appels audio et vidéo d'Apple. À l'instar d'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 au moyen d'un chiffrement de bout en bout qui interdit l'accès à toute autre personne que l'expéditeur et le destinataire. Apple n'est pas en mesure de déchiffrer ces données.

La connexion FaceTime initiale se fait au moyen de l'infrastructure des serveurs Apple qui relaient les paquets de données entre les appareils enregistrés des utilisateurs. Les appareils vérifient leurs certificats d'identification à l'aide de notifications APN et de messages STUN pour NAT, et établissent un secret partagé pour chaque session. Le secret partagé est utilisé pour extraire 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 des chiffrements AES-256 en mode compteur et HMAC-SHA1. À la suite de la connexion initiale et de la configuration de sécurité, FaceTime utilise STUN et ICE (Internet Connectivity Establishment) pour établir une connexion poste-à-poste entre les appareils, si possible.

FaceTime en groupe permet de passer des appels qui comptent jusqu'à 33 correspondants simultanément. Tout comme lors des 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 l'infrastructure et le design de FaceTime en tête-à-tête soient réutilisés, les appels FaceTime en groupe reposent sur un nouveau mécanisme d'assignation de clés qui s'ajoute à l'authenticité fournie par l'IDS. Ce protocole est source de confidentialité persistante. Cela signifie 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.

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'application 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. Les fonctionnalités iCloud, telles que Mon flux de photos, iCloud Drive et Sauvegarde iCloud, peuvent être désactivées par des administrateurs informatiques au moyen de profils de configuration de 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 au moyen du protocole AES-128 et d'une clé obtenue à partir du contenu de chaque bloc utilisant le protocole SHA-256. 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 les services Web d'Amazon ou la plateforme Google Cloud. Ces partenaires ne possèdent pas les clés pour déchiffrer les données stockées sur leurs serveurs.

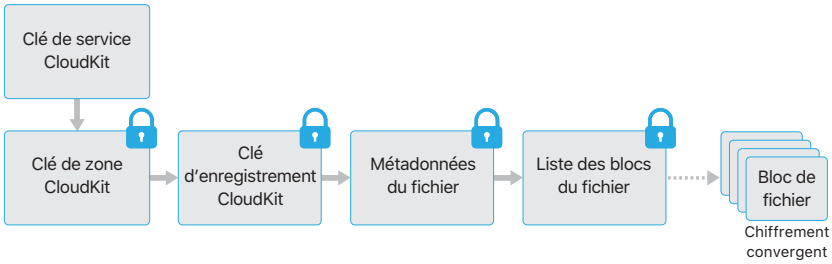
iCloud Drive

iCloud Drive ajoute des clés basées sur le compte pour protéger les documents enregistrés dans iCloud. Comme pour les autres services iCloud, il divise le contenu des fichiers en plusieurs blocs qu'il chiffre avant de stocker les 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 qui est ensuite stockée avec le compte iCloud de l'utilisateur. 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.

CloudKit

CloudKit permet aux développeurs d'apps d'enregistrer des données de valeur de clé, 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 le font 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 de 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

Plusieurs services Apple, répertoriés dans l'article « Présentation de la sécurité iCloud » de l'Assistance Apple (https://support.apple.com/HT202303), 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 partage ses caractéristiques de sécurité; les clés sont accessibles uniquement par les appareils autorisés par l'utilisateur et non par Apple ou un tiers. Si l'accès aux données du trousseau iCloud est perdu (voir la section « Sécurité du dépôt » plus loin dans ce document), les données dans CloudKit sont réinitialisées, et, si des données sont accessibles sur l'appareil local autorisé, elles sont téléchargées de nouveau vers CloudKit.

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 de confiance. Cette clé de service iCloud est renouvelée lorsque l'utilisateur désactive la sauvegarde iCloud.

Sauvegarde iCloud

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) via Wi-Fi. iCloud protège le contenu en le chiffrant lorsqu'il est envoyé via 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

Options de récupération

Situation	Options de récupération de l'utilisateur pour le chiffrement de bout en bout CloudKit
Accès à un appareil de confiance	Récupération des données possible via l'appareil de confiance ou le trousseau iCloud.
Aucun appareil de confiance	Récupération des données possible uniquement via le trousseau iCloud.

Situation	Options de récupération de l'utilisateur pour Messages dans iCloud
Sauvegarde iCloud activée et accès à un appareil de confiance	Récupération des données possible via la sauvegarde iCloud, l'appareil de confiance ou le trousseau iCloud.
Sauvegarde iCloud activée; aucun appareil de confiance	Récupération des données possible via la sauvegarde iCloud ou le trousseau iCloud.
Sauvegarde iCloud désactivée et accès à un appareil de confiance	Récupération des données possible via l'appareil de confiance ou le trousseau iCloud.
Sauvegarde désactivée; aucun appareil de confiance	Récupération des données possible uniquement via le trousseau iCloud.

l'entremise d'un réseau Wi-Fi. En raison du type de chiffrement utilisé dans iOS, le système est conçu pour protéger les données tout en autorisant des sauvegardes et des restaurations incrémentales et sans surveillance.

Données sauvegardées par iCloud :

- Données sur la musique, les vidéos, les émissions, les apps et les livres. La sauvegarde iCloud d'un utilisateur inclut des informations sur le contenu acheté présent son appareil iOS, mais pas le contenu acheté en soi. 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 ou d'Apple Books. Certains types de contenus ne sont pas téléchargés automatiquement dans tous les pays ou toutes les 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 iOS de l'utilisateur. Notez que si l'utilisateur active la photothèque iCloud sur son appareil iOS (iOS 8.1 ou version ultérieure) ou Mac (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.
- Historique des appels et sonneries.
- Écran d'accueil et organisation des apps.
- Configuration de HomeKit.
- Données HealthKit.
- Mot de passe de la messagerie vocale visuelle (nécessite la carte SIM utilisée au moment de la sauvegarde).
- iMessage, clavardage d'entreprise, messages texte (SMS) et messages MMS (nécessite la carte SIM utilisée au moment de la sauvegarde).

  Remarque : Lorsque Messages est activée dans iCloud, iMessage, le clavardage d'entreprise 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.

Si des fichiers sont créés dans des classes de protection de données inaccessibles lorsque l'appareil est verrouillé, leurs clés de fichier sont chiffrées à l'aide des clés de classe provenant du conteneur de clés de Sauvegarde iCloud. Les fichiers sont sauvegardés sur iCloud dans leur état chiffré d'origine. Les fichiers de la classe de protection de données Aucune protection sont chiffrés durant le transfert.

Le conteneur de clés de Sauvegarde iCloud contient des clés asymétriques (Curve25519) pour chaque classe de protection de données, qui sont utilisées pour chiffrer les clés de fichier. Pour en savoir plus sur le contenu du conteneur de clés de sauvegarde et sur le conteneur de clés

de Sauvegarde iCloud, reportez-vous à la sous-section « Protection des données du trousseau » de la section « Chiffrement et protection des données » du présent document.

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 Sauvegarde iCloud. Le conteneur de clés de Sauvegarde iCloud 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 entremêlée avec l'UID. Cela permet de restaurer le trousseau uniquement sur son appareil d'origine afin qu'aucune autre personne (y compris Apple) n'ait accès aux éléments du trousseau de l'utilisateur.

Lors de la restauration, les fichiers sauvegardés, le conteneur de clés de Sauvegarde iCloud et la clé du conteneur de clés sont récupérés à partir du compte iCloud de l'utilisateur. Le conteneur de clés de Sauvegarde iCloud est déchiffré au moyen de sa clé; les clés de fichier du conteneur de clés 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.

Trousseau iCloud

Intégration de Safari au trousseau iCloud
Safari peut générer automatiquement des chaînes de caractères aléatoires et solides au plan cryptographique comme mots de passe de sites web. Elles sont ensuite stockées dans le trousseau et synchronisées avec les autres appareils de l'utilisateur. 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.

Le trousseau iCloud donne aux utilisateurs la possibilité de synchroniser de façon sécurisée leurs mots de passe avec plusieurs appareils iOS 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 de trousseaux et la récupération de trousseau.

Apple a conçu le trousseau iCloud et la récupération de 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 de l'utilisateur.

Synchronisation de trousseaux

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 (salage et itérations aléatoires) sont également stockés avec le cercle.

Le cercle de synchronisation signé est ensuite placé dans la zone de stockage des valeurs de clé 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, ce dernier 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'identification 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.

Lorsque le premier appareil constate qu'un ticket de candidature est arrivé, il affiche un message invitant l'utilisateur à 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. Cela permet d'établir que la personne à l'origine de la demande d'entrée dans le cercle a saisi le mot de passe iCloud de l'utilisateur au moment de la requête.

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 via l'espace de stockage des valeurs de clé iCloud ou à les stocker dans CloudKit, selon le cas. 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 autorisé par l'utilisateur. Il ne peut pas être déchiffré par d'autres appareils ni par 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. Il peut alors approuver le nouveau membre à partir de l'un de ces deux appareils. À mesure que de nouveaux appareils sont ajoutés, chaque appareil est synchronisé avec le nouveau pour s'assurer que tous les membres disposent des mêmes éléments de trousseau.

La totalité du trousseau n'est toutefois pas synchronisée. Certains éléments sont propres à chaque appareil, tels que les identités VPN, et ne devraient pas quitter leur appareil. 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 bancaire) 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 de tiers ne sont pas synchronisés par défaut. Les développeurs doivent définir l'attribut `kSecAttrSynchronizable` lorsqu'ils ajoutent des éléments au trousseau.

Récupération de trousseau

La récupération de trousseau offre aux utilisateurs qui le souhaitent un moyen de confier leur trousseau à Apple sans permettre à Apple de lire les mots de passe et autres données qu'il contient. La récupération de trousseau fournit 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 complexes et aléatoires pour des comptes web, car le trousseau constitue le seul endroit où sont enregistrés ces mots de passe.

La récupération de trousseau repose sur l'authentification secondaire et sur un service de dépôt sécurisé 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 de dépôt fournit une copie du trousseau uniquement si certaines conditions strictes sont remplies.

Lorsque le trousseau iCloud est activé, si l'authentification à deux facteurs est activée pour le compte de l'utilisateur, le code de l'appareil sera utilisé pour récupérer un trousseau en dépôt. 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.

L'appareil iOS exporte ensuite une copie du trousseau de l'utilisateur, chiffre cette copie en l'enveloppant avec des clés dans un conteneur de clés asymétrique et la place dans la zone de stockage des valeurs de clé 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 HSM (module de sécurité matériel) destinée à stocker l'enregistrement en dépôt. Ce dernier devient alors l'enregistrement en dépôt iCloud de l'utilisateur.

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 en dépôt n'est nécessaire. Au lieu de cela, le code de sécurité iCloud est utilisé pour protéger directement la clé aléatoire.

En plus d'établir un code de sécurité, les utilisateurs doivent enregistrer un numéro de téléphone. Ce numéro offre un deuxième niveau d'authentification lors de la récupération d'un trousseau. L'utilisateur reçoit un message texte auquel il doit répondre pour que la récupération soit effectuée.

Sécurité du dépôt

iCloud offre une infrastructure de sécurité pour le dépôt de trousseau qui permet de garantir que seuls des utilisateurs et des appareils autorisés peuvent effectuer la récupération. Les grappes HSM sont topographiquement placées derrière iCloud pour protéger les enregistrements en dépôt. Chacun d'eux possède une clé utilisée pour chiffrer les enregistrements en dépôt placés sous sa garde (voir description précédente).

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. Après avoir effectué cette opération, ils doivent également saisir leur code de sécurité iCloud.

La grappe HSM vérifie que l'utilisateur connaît son code de sécurité iCloud via le 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 grappes, l'enregistrement en dépôt 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. Grâce à cette clé, le trousseau (récupéré à partir de l'espace de stockage des valeurs de clé iCloud) est déchiffré et restauré sur l'appareil. Le nombre de tentatives d'authentification et de récupération d'un enregistrement en dépôt est fixé à dix. Après plusieurs tentatives manquées, l'enregistrement est verrouillé et l'utilisateur doit appeler l'assistance Apple pour pouvoir effectuer des tentatives supplémentaires. Après la dixième tentative manquée, la grappe HSM détruit l'enregistrement en dépôt, 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 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 cette dernière par la grappe HSM. Dans ce cas, les propriétaires de chaque trousseau protégé par la grappe reçoivent un message leur annonçant la perte de leur enregistrement placé en dépôt. Ils peuvent alors décider de se réinscrire au service.

Siri

Les utilisateurs peuvent, en parlant naturellement, demander à Siri d'envoyer des messages, de programmer des rendez-vous, d'effectuer des appels téléphoniques et bien plus encore. Siri fait appel à la reconnaissance vocale, à la synthèse vocale et à un modèle client-serveur pour répondre à un large éventail de questions. Les tâches prises en charge par Siri ont été conçues pour n'utiliser qu'une quantité absolument minimale de données personnelles et assurer une protection totale de celles-ci.

Lorsque Siri est activé, l'appareil crée des identifiants aléatoires qui sont utilisés avec les serveurs Siri et les serveurs de reconnaissance vocale. Ces identifiants sont utilisés exclusivement dans Siri et servent à améliorer le service. Lorsque Siri est ensuite désactivé, l'appareil génère un nouvel identifiant aléatoire à utiliser au moment de la réactivation de Siri.

Pour permettre la mise en œuvre des fonctionnalités de Siri, certaines données d'utilisateur présentes sur l'appareil sont envoyées au serveur. Cela comprend notamment les données de la bibliothèque musicale (titres des chansons, artistes et listes de lecture), les noms des listes de rappels ainsi que les noms et les relations définis dans Contacts. Toutes les communications avec le serveur sont effectuées via HTTPS.

Lorsqu'une session Siri est lancée, le nom et le prénom de l'utilisateur (provenant de Contacts) ainsi que sa position géographique approximative sont envoyés au serveur. Cela permet à Siri de s'adresser à l'utilisateur par son nom ou de répondre à des questions ne nécessitant qu'une position approximative, comme la météo par exemple.

Si une position plus précise est nécessaire, pour indiquer les salles de cinéma les plus proches par exemple, le serveur demande à l'appareil de lui fournir une position plus précise. Cela montre comment, par défaut, l'information est envoyée au serveur uniquement lorsque cela s'avère strictement nécessaire pour traiter la demande de l'utilisateur. Les informations de session sont éliminées après dix minutes d'inactivité, quoi qu'il arrive.

Lorsque Siri est utilisé à partir d'une Apple Watch, cette dernière crée son propre identifiant unique aléatoire, comme décrit précédemment. Toutefois, au lieu d'envoyer à nouveau les informations de l'utilisateur, ses requêtes intègrent également l'identifiant Siri de l'iPhone jumelé pour fournir une référence à ces informations.

L'enregistrement des phrases prononcées par l'utilisateur est envoyé au serveur de reconnaissance vocale d'Apple. Si la tâche n'implique qu'une simple dictée, le texte reconnu est renvoyé à l'appareil. Sinon, Siri analyse le texte et, si nécessaire, le combine avec des informations provenant du profil associé à l'appareil. Si la demande est « envoyer un message à ma mère », par exemple, les relations et les noms téléchargés à partir de Contacts sont utilisés. La commande de l'action identifiée est ensuite renvoyée à l'appareil afin d'être exécutée.

De nombreuses actions de Siri sont effectuées par l'appareil sous les instructions du serveur. Par exemple, si l'utilisateur demande à Siri de lire un message entrant, le serveur demande simplement à l'appareil de lire le contenu de ses messages non lus à voix haute. Le contenu et l'expéditeur du message ne sont pas envoyés au serveur.

Les enregistrements vocaux de l'utilisateur sont conservés pendant six mois afin que le système de reconnaissance vocale puisse les utiliser pour mieux comprendre la voix de l'utilisateur. Une autre copie est enregistrée après six mois, sans son identifiant afin qu'Apple puisse l'utiliser pour améliorer et développer Siri, et ce, pendant deux ans au total. Un petit sous-ensemble d'enregistrements, de transcriptions et de données associées sans identifiant pourrait continuer d'être utilisé par Apple pour favoriser l'amélioration continue et l'assurance de la qualité de Siri au-delà de deux ans. De plus, certains enregistrements faisant référence à la musique, aux équipes sportives et à leurs joueurs, ainsi qu'au monde des affaires et aux points d'intérêt sont enregistrés de la même manière en vue d'améliorer le service Siri.

Il est également possible d'utiliser Siri en mode mains libres au moyen de l'activation vocale. La détection de commande vocale est effectuée localement sur l'appareil. Avec ce mode, Siri n'est activé que si les mots entendus correspondent de manière satisfaisante au profil acoustique de la commande vocale spécifiée. Lorsque la commande est détectée, le son correspondant incluant la commande Siri est envoyé au serveur de reconnaissance vocale d'Apple en vue d'un traitement supplémentaire, selon les mêmes règles que celles appliquées aux autres enregistrements vocaux effectués via Siri.

Les utilisateurs peuvent également appeler Siri sur l'Apple Watch en levant leur poignet près de leur bouche avant d'énoncer une demande Siri. Siri est activée de cette manière aux conditions suivantes :

- un modèle d'apprentissage machine sur l'appareil détecte une voix humaine près de l'appareil;
- un deuxième modèle d'apprentissage machine identifie un profil de mouvement et que la position de l'appareil correspond au geste Lever pour parler.

Lorsque cette combinaison de geste et de son est détectée, le son correspondant est envoyé au serveur de reconnaissance vocale d'Apple en vue d'un traitement supplémentaire, selon les mêmes règles que celles appliquées aux autres enregistrements vocaux effectués via Siri.

Suggestions de Siri

Les suggestions de Siri pour les apps et les raccourcis sont générées à l'aide de l'apprentissage machine sur l'appareil. Aucune donnée n'est transmise à Apple à l'exception des informations qui ne peuvent pas être utilisées pour identifier l'utilisateur concernant les signaux qui ont prédit de manière utile les raccourcis et les apps lancées.

Raccourcis dans Siri

Les raccourcis ajoutés à Siri sont synchronisés sur tous les appareils Apple qui utilisent iCloud et chiffrés par chiffrement bout en bout CloudKit. Les phrases associées aux raccourcis sont synchronisées avec le serveur Siri aux fins de reconnaissance vocale, et associées avec l'identifiant Siri aléatoire décrit précédemment dans cette section. Les raccourcis sont stockés localement dans une voûte de données et Apple n'en reçoit pas le contenu.

App Raccourcis

Les raccourcis personnalisés dans l'app Raccourcis sont facultativement synchronisés avec tous les appareils Apple à l'aide d'iCloud. Les raccourcis peuvent également être partagés avec d'autres utilisateurs par iCloud.

Les raccourcis personnalisés sont polyvalents, comme des scripts ou des programmes. Un système de quarantaine est utilisé pour isoler les raccourcis téléchargés sur internet. L'utilisateur est averti la première fois qu'il tente d'utiliser le raccourci et il a alors l'occasion de l'inspecter, y compris les renseignements sur son origine.

Les raccourcis personnalisés peuvent également exécuter du JavaScript précisé par l'utilisateur sur les sites web dans Safari lorsqu'ils sont invoqués depuis la feuille de partage. À titre de protection contre le JavaScript malveillant qui, par exemple, amène l'utilisateur à exécuter un script sur un site de médias sociaux qui recueille ses données, des définitions à jour de logiciels malveillants sont téléchargées pour identifier les scripts malveillants au moment de l'exécution. La première fois qu'un utilisateur exécute du 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.

Suggestions de Safari, suggestions de Siri dans Rechercher, Chercher, #images, app et widget News dans les pays où News n'est pas disponible

Suggestions de Safari, suggestions de Siri dans Rechercher, Chercher, #images et le widget News (dans les pays où News n'est pas disponible) affichent des suggestions qui vont au-delà de l'appareil, à partir de sources comme Wikipédia, l'iTunes Store, les nouvelles locales, les résultats de Plans et l'App Store. Ils proposent des suggestions avant même que l'utilisateur commence à effectuer une saisie.

Lorsqu'un utilisateur commence à taper dans la barre d'adresse de Safari, ouvre ou utilise les suggestions de Siri dans Rechercher, utilise Chercher, ouvre #images, utilise Rechercher dans l'app News ou utilise le widget News dans un pays où News n'est pas disponible, le contexte suivant est envoyé à l'aide de HTTPS à Apple afin de fournir des résultats pertinents à l'utilisateur :

- un identifiant qui change toutes les 15 minutes pour conserver la confidentialité;
- la requête de recherche de l'utilisateur;
- la requête la plus probable selon le contexte et les recherches antérieures mises en cache localement;
- l'emplacement approximatif de l'appareil, l'option Suggestions selon le lieu du Service de localisation est activée. Le niveau d'« approximation » de la localisation dépend de la densité de population estimée à l'endroit où se trouve l'appareil; ce niveau est plus important dans les zones rurales, où les utilisateurs tendent à être géographiquement plus éloignés que dans les zones urbaines, où les utilisateurs sont généralement plus proches les uns des autres. Les utilisateurs ont la possibilité de désactiver l'envoi à Apple de toutes les données de position géographique en désactivant l'option Suggestions selon le lieu du Service de localisation. Si le Service de localisation est désactivé, Apple peut utiliser l'adresse IP de l'appareil pour inférer une position approximative;
- le type d'appareil et l'origine de la recherche (suggestions de Siri dans Rechercher, Safari, Chercher, l'app News ou Messages);
- le type de connexion;
- les informations sur les trois dernières apps utilisées (pour fournir un contexte de recherche supplémentaire). Seules les apps reprises dans une liste blanche tenue à jour par Apple et contenant les apps populaires utilisées au cours des trois dernières heures sont incluses;
- une liste des applications populaires sur l'appareil;
- la langue régionale, les paramètres régionaux et les préférences d'entrée;
- si l'appareil de l'utilisateur peut accéder aux services d'abonnement de musique ou de vidéo, les informations, telles que les noms des services d'abonnement et les types d'abonnements, peuvent être envoyées à Apple. Le nom, le numéro et le mot de passe du compte ne sont pas envoyés à Apple;
- la représentation abrégée et compilée des sujets d'intérêt.

Lorsqu'un utilisateur sélectionne un résultat ou ferme l'app sans rien avoir sélectionné, des informations sont envoyées à Apple pour contribuer à améliorer la qualité des résultats futurs. Ces informations sont liées uniquement au même identifiant de session de 15 minutes et non à un utilisateur particulier. La rétroaction comprend les informations de contexte mentionnées ci-dessus ainsi que les informations suivantes liées aux interactions :

- la durée entre les interactions et les demandes de recherche de réseau;
- le classement et l'ordre d'affichage des suggestions;
- l'identifiant du résultat et l'action sélectionnée si le résultat n'est pas local, ou la catégorie du résultat s'il est local;
- un drapeau indiquant si l'utilisateur a sélectionné le résultat.

Apple conserve pendant 18 mois au maximum les historiques de Suggestions comprenant les requêtes, le contexte et la rétroaction. Un sous-ensemble des historiques est conservé pendant cinq ans au maximum, comme les requêtes, les paramètres régionaux, le domaine, l'emplacement approximatif et les mesures consolidées.

Dans certains cas, Suggestions peut transférer des requêtes relatives à des phrases et des mots courants à un partenaire agréé afin de recevoir et d'afficher les résultats de recherche de ce partenaire. Apple fait office de serveur de procuration pour les requêtes, de sorte que les partenaires ne reçoivent pas les adresses IP ou les rétroactions de recherche des utilisateurs. La communication avec le partenaire est chiffrée par HTTPS. Pour les requêtes qui ont lieu fréquemment, Apple fournit au partenaire la ville, le type d'appareil et la langue du client comme contexte de recherche afin d'améliorer les résultats de recherche.

Les informations suivantes sont enregistrées sans identifiant de session pour permettre de comprendre et d'améliorer les performances dans différentes régions et sur divers types de réseaux :

- l'adresse IP partielle (sans le dernier octet des adresses IPv4, sans les 80 derniers bits pour les adresses IPv6);
- l'emplacement approximatif;
- l'heure approximative de la requête;
- la latence ou la fréquence de transfert;
- la taille de la réponse;
- le type de connexion;
- les paramètres régionaux;
- le type d'appareil et l'app de requête.

Contrôle intelligent du suivi dans Safari

Le contrôle intelligent du suivi fait partie de la politique relative aux données des sites web et aux témoins par défaut de Safari visant la protection de la vie privée. Elle aide à prévenir le suivi entre sites en limitant l'accès aux témoins et aux autres données des sites web.

L'ITP recueille des statistiques sur les chargements de ressources (images, scripts, etc.) ainsi que sur les interactions des utilisateurs comme les touchers et les saisies de texte. Un modèle d'apprentissage machine est utilisé pour la classification sur l'appareil des noms de domaines ayant la capacité de suivre l'utilisateur entre les sites, selon les statistiques recueillies.

Lorsqu'un domaine est classifié comme ayant des capacités de suivi, l'ITP partitionne immédiatement ses témoins si l'utilisateur a déjà interagi directement avec ce domaine; pour les domaines classifiés avec lesquels l'utilisateur n'a pas eu d'interaction, l'ITP commence immédiatement à bloquer ses témoins. Par exemple :

- video.example offre un service d'abonnement sans publicité et plusieurs de ses vidéos sont intégrées sur d'autres sites web.
- Un utilisateur se connecte à video.example, puis accède à d'autres sites web contenant du contenu intégré de video.example.
- L'ITP classifie video.example comme ayant des capacités de suivi et partitionne donc ses témoins.
- Lorsqu'un utilisateur visite newspaper.example et qu'il contient du contenu intégré de video.example, les témoins fournis à video.example sont partitionnés et concernent exclusivement video.example sur newspaper.example.

Le contenu tiers intégré peut demander à un utilisateur d'avoir accès à ses témoins de première partie avec l'API d'accès au stockage. Lorsqu'un utilisateur touche à du contenu de tiers intégré qui utilise l'API d'accès au stockage, ou qu'il clique dessus, Safari affiche un message demandant à l'utilisateur s'il souhaite autoriser le tiers à accéder à ses témoins et à ses données de site web, ce qui permet à ce tiers de le suivre sur le domaine de première partie. Si l'utilisateur choisit Autoriser, le contenu tiers intégré est autorisé à accéder à ses témoins de première partie pendant la durée de la visite de la page; lors des visites ultérieures, le contenu tiers intégré aura accès à ses témoins de première partie après l'interaction de l'utilisateur avec le contenu intégré qui déclenche l'appel de l'API d'accès au stockage. De plus, puisque l'utilisateur a déjà autorisé cet accès, il n'est pas interrogé de nouveau. La décision de l'utilisateur est conservée pour la combinaison des première et tierce parties, et elle est effacée lorsque l'utilisateur vide son historique de Safari.

Les témoins existants de domaines classifiés comme ayant des capacités de suivi sont éliminés si l'utilisateur n'a pas interagi avec ce domaine, directement ou par l'API d'accès au stockage, pendant 30 jours d'utilisation active de Safari. Après 30 jours sans interaction, un domaine classifié comme ayant des capacités de suivi ne peut pas non plus configurer de nouveaux témoins. Safari n'autorise jamais l'accès aux données de sites web de première partie dans des contextes tiers.

L’isolation de l’ITP des données de première et de tierce parties permet d’empêcher l’utilisation des témoins et des données de sites web aux fins de suivi entre les sites. Apple n’a pas accès aux noms des domaines au sujet desquels un appareil a recueilli des statistiques ou qui ont été classifiés comme ayant des capacités de suivi.

En plus de bloquer les témoins tiers des domaines classifiés comme ayant des capacités de suivi, l’ITP limite également les renseignements sur le référent HTTP envoyés à ces domaines tiers classifiés à l’origine de la page.

Gestion des mots de passe d’utilisateur

iOS offre de nombreuses fonctionnalités pour permettre aux utilisateurs de pouvoir authentifier les apps et les sites web tiers qui utilisent des mots de passe pour l’authentification de manière simple, sécuritaire et pratique. 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 et comptes > Mots de passe (web/apps). Les apps ne peuvent pas accéder au trousseau de remplissage automatique des mots de passe sans l’autorisation de l’utilisateur. Les informations d’identification enregistrées dans le trousseau de remplissage automatique des mots de passe sont synchronisées entre les appareils avec le trousseau iCloud s’il est activé.

Le gestionnaire de mots de passe du trousseau iCloud et le remplissage automatique des mots de passe offre 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 par les contacts de l’utilisateur;
- transmission des mots de passe à une Apple TV à proximité qui demande des informations d’identification.

Accès des apps aux mots de passe enregistrés

API d’informations d’identification web partagées

Les apps iOS peuvent interagir avec les éléments du trousseau de remplissage automatique des mots de passe à l’aide des deux API suivantes :

- `SecRequestSharedWebCredential`
- `SecAddSharedWebCredential`

L’accès n’est accordé aux apps iOS que 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 un droit dans leur app. Ce droit 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 envoie 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 marque 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.

Remplissage automatique des mots de passe pour les apps

iOS permet aux utilisateurs d'introduire des noms d'utilisateur et des mots de passe dans les champs d'identification des apps à l'aide des « touches » à capacité suggestive d'action de la barre QuickType du clavier iOS. Il utilise le même mécanisme d'association app et site web alimenté par le fichier apple-app-site-association pour associer avec certitude les apps et les sites web. Cette interface n'expose aucune information d'identification à l'app avant que l'utilisateur accepte d'en transmettre à l'app. Lorsqu'iOS signale une relation de confiance entre un site web et une app, la barre QuickType suggère directement les informations d'identification à transmettre à l'app. Cela permet aux utilisateurs de choisir de divulguer les informations d'identification enregistrées dans Safari aux apps qui partagent les mêmes propriétés de sécurité, mais sans que les apps aient à adopter une API.

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 peut demander à l'utilisateur d'enregistrer ces informations dans le trousseau de remplissage automatique des mots de passe pour les utiliser plus tard.

Mots de passe robustes automatiques

Lorsque le trousseau iCloud est activé, iOS crée des mots de passe robustes, aléatoires et uniques lorsque les utilisateurs s'inscrivent ou qu'ils modifient leur mot de passe dans une app ou sur un site web dans Safari. Les utilisateurs doivent eux-mêmes désactiver l'utilisation de mots de passe robustes. 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.

Les mots de passe générés par iOS par défaut contiennent vingt caractères. Ils contiennent un chiffre, une majuscule, deux traits d'union et seize minuscules. Ces mots de passe générés sont robustes, comportant une entropie de 71 bits.

iOS générera les mots de passe des apps et dans Safari selon une heuristique qui détermine que l'expérience d'un champ de mot de passe est pour sa création. Si l'heuristique ne reconnaît pas le contexte d'un mot de passe comme étant pour sa création, les développeurs de l'app peuvent régler UITextContentType.newPassword dans leur champ de texte et les développeurs web peuvent indiquer autocomplete="new-password" dans leurs éléments <input>.

Les apps et les sites web peuvent fournir des règles à iOS pour s'assurer que les mots de passe générés sont compatibles avec les services pertinents. iOS générera le mot de passe le plus robuste possible qui respecte ces règles. Les développeurs fournissent ces règles à l'aide du réglage UITextInputPasswordRules ou de l'attribut passwordrules dans leurs éléments <input>.

Envoi de mots de passe à d'autres personnes ou appareils

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'utilisation. (Voir la section « Sécurité AirDrop » pour en savoir plus.) Sur l'appareil récepteur, après le consentement de l'utilisateur, les informations d'identification seront stockées dans le trousseau de remplissage des mots de passe de l'utilisateur.

Apple TV

Le remplissage automatique des mots de passe est disponible pour remplir les informations d'identification dans les apps sur l'Apple TV. Lorsque l'utilisateur sélectionne un champ de texte pour un nom d'utilisateur ou un mot de passe dans tvOS, l'Apple TV commence à interroger le remplissage automatique des mots de passe par Bluetooth Low Energy (BLE).

Tout iPhone à proximité affiche un message invitant l'utilisateur à partager ses informations d'identification avec l'Apple TV. Un iPhone et une Apple TV qui utilisent le même compte iCloud chiffrent la communication entre les deux appareils au cours de ce processus. Si l'iPhone est connecté à un compte iCloud différent de celui de l'Apple TV :

- un code NIP est utilisé pour établir une connexion chiffrée;
- l'iPhone doit être déverrouillé et à proximité de la télécommande Siri Remote jumelée à cette Apple TV pour recevoir ce message.

Après l'établissement de la connexion chiffrée à l'aide du chiffrement de lien Bluetooth LE, 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

Les utilisateurs peuvent désigner une application tierce conforme comme fournisseur d'informations d'identification au remplissage dans les réglages Mots de passe et comptes. Ce mécanisme est fondé sur des extensions. L'extension de fournisseurs d'informations d'identification doit fournir un affichage pour la sélection des informations et elle peut facultativement fournir des métadonnées iOS au sujet des informations enregistrées afin qu'elles puissent être offertes directement dans la barre QuickType. Les métadonnées comprennent le site web pour les informations d'identification et le nom d'utilisateur associé, mais pas son mot de passe. iOS communiquera avec l'extension pour obtenir le mot de passe lorsque l'utilisateur choisit de le remplir dans une application ou sur un site web dans Safari. Les métadonnées des informations d'identification sont stockées dans le bac à sable du fournisseur et elles sont automatiquement supprimées lorsqu'une app est désinstallée.

Contrôles de l’appareil

La plateforme iOS prend en charge des politiques et des configurations de sécurité souples, faciles à appliquer et à gérer. Cela permet aux organisations de protéger leurs informations et de s’assurer que les employés respectent les exigences de l’entreprise même s’ils utilisent leurs propres appareils dans le cadre d’un programme d’utilisation de matériel personnel au travail, par exemple.

Les organisations peuvent utiliser des moyens comme la protection par code, les profils de configuration, l’effacement à distance ou des solutions de gestion d’appareils mobiles (GAM) de tiers pour gérer leurs parcs d’appareils et garantir la sécurité de leurs données, même si leurs employés accèdent à celles-ci sur leurs propres appareils iOS.

Protection par code

Par défaut, le mot de passe est un numéro d’identification personnel. Sur les appareils dotés de Touch ID ou de Face ID, la longueur minimale du code est de quatre chiffres. Les utilisateurs peuvent indiquer un code alphanumérique plus long en sélectionnant Code alphanumérique personnalisé dans les Options de code de Réglages > Touch ID et code. Les codes plus complexes ou plus longs sont plus difficiles à deviner ou à attaquer et sont recommandés.

Les administrateurs peuvent imposer l’utilisation de codes complexes et d’autres politiques, soit à l’aide d’Exchange ActiveSync ou d’une solution de GAM, soit en demandant aux utilisateurs d’installer manuellement des profils de configuration. Il existe plusieurs possibilités en matière de politiques de code :

- valeurs simples permises;
- valeurs alphanumériques obligatoires;
- longueur de code minimum;
- nombre minimum de caractères complexes;
- période d’utilisation maximale;
- historique des codes;
- délai de blocage automatique;
- période de grâce pour le blocage de l’appareil;
- nombre maximum de tentatives manquées;
- autorisation de Touch ID ou de Face ID.

Pour obtenir des informations destinées aux administrateurs au sujet de chaque politique, rendez-vous sur : https://support.apple.com/fr-ca/guide/mdm/

Pour obtenir des informations destinées aux développeurs au sujet de chaque politique, rendez-vous sur : https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf

Modèle de jumelage iOS

iOS utilise 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 utilise cette marque de confiance pour activer des fonctionnalités supplémentaires avec l'hôte connecté, comme la synchronisation de données.

Dans iOS 9, les services qui nécessitent un jumelage ne peuvent pas être lancés tant que l'appareil n'a pas été déverrouillé par l'utilisateur.

De plus, dans iOS 10 ou version ultérieure, certains services, y compris la synchronisation des photos, requièrent que l'appareil soit déverrouillé pour commencer.

Dans iOS 11 ou version ultérieure, les services ne démarreront pas à moins que l'appareil ait été déverrouillé récemment.

Le processus de jumelage nécessite que l'utilisateur déverrouille l'appareil et accepte la demande de jumelage émise par l'hôte. Dans iOS 11 ou version ultérieure, l'utilisateur doit également entrer son code. Une fois que l'utilisateur a accepté cette demande, l'hôte et l'appareil échangent et enregistrent des clés publiques RSA 2 048 bits. L'hôte reçoit ensuite une clé 256 bits capable de débloquer un conteneur de clés en dépôt sur l'appareil (voir la partie consacrée aux conteneurs de clés en dépôt dans la section « Conteneurs de clés » du présent document). 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 iTunes, transferts de fichiers, développement Xcode, etc.). Comme l'appareil nécessite des connexions via Wi-Fi à partir d'un hôte pour utiliser cette session chiffrée pour toutes les communications, il faut qu'il ait été précédemment jumelé via USB. Le jumelage permet aussi d'activer plusieurs capacités de diagnostic. Dans iOS 9, si la fiche d'un jumelage n'a pas été utilisée pendant plus de six mois, elle expire. Cette période est raccourcie à 30 jours dans iOS 11 ou version ultérieure.

Pour obtenir plus d'informations, rendez-vous sur :
https://support.apple.com/HT203034

Certains services, comme com.apple.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.

Dans iOS 11 ou version ultérieure, l'Apple TV peut avoir recours au protocole SRP afin d'établir un jumelage sans fil.

L'utilisateur peut effacer la liste des hôtes de confiance à l'aide des options « Réinitialiser les réglages réseau » ou « Réin. localisation et confidentialité ».

Pour obtenir plus d'informations, rendez-vous sur :
https://support.apple.com/HT202778

Application de la configuration

Un profil de configuration est un fichier XML qui permet à un administrateur de distribuer des informations de configuration à des appareils iOS. Les réglages définis par un profil de configuration installé ne peuvent être modifiés par l'utilisateur. Si l'utilisateur supprime un profil de configuration, tous les réglages définis par le profil sont également supprimés. Les administrateurs peuvent ainsi appliquer des réglages en associant des politiques à l'accès Wi-Fi et à l'accès aux données. Un profil de configuration destiné à fournir une configuration de courriel, par exemple, peut également spécifier une politique de code pour un appareil. Les utilisateurs ne pourront accéder à leur courrier électronique que si leur code est conforme aux exigences de l'administrateur.

Dans les profils de configuration iOS, plusieurs réglages peuvent être modifiés :

- politiques en matière de code;
- restrictions liées aux fonctionnalités de l'appareil (comme la désactivation de la caméra);
- réglages Wi-Fi;
- réglages VPN;
- réglages de serveur de courrier;
- réglages Exchange;
- réglages de service de répertoire LDAP;
- réglages de service de calendrier CalDAV;
- clips web;
- accréditations et clés;
- réglages avancés de réseau cellulaire.

Pour voir la liste actualisée destinée aux administrateurs, rendez-vous sur : https://support.apple.com/fr-ca/guide/mdm/mdm5370d089

Pour voir la liste actualisée destinée aux développeurs, rendez-vous sur : https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf

Il est possible de signer et de chiffrer les profils de configuration afin de valider leur origine, de garantir leur intégrité et de protéger leur contenu. Les profils de configuration sont chiffrés avec la syntaxe CMS (RFC 3852), qui prend en charge les algorithmes 3DES et AES-128.

Il est également possible de verrouiller des profils de configuration sur un appareil afin d'interdire complètement leur suppression ou de n'autoriser cette dernière qu'au moyen d'un code. Comme beaucoup d'utilisateurs professionnels possèdent leurs propres appareils iOS, 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.

Les utilisateurs peuvent installer des profils de configuration directement sur leurs appareils à l'aide d'Apple Configurator 2, en télécharger via Safari, se les faire envoyer par courrier électronique ou les recevoir via une connexion sans fil à partir d'une solution de 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.

Gestion des appareils mobiles (GAM)

La prise en charge de la gestion des appareils mobiles (GAM) par iOS permet aux entreprises de gérer et de configurer de manière sécurisée des déploiements d'iPhone, d'iPad, d'Apple TV et de Mac à grande échelle dans toute leur organisation. Les fonctionnalités de GAM sont intégrées aux technologies iOS existantes, comme les profils de configuration, l'inscription sans fil et le service Apple de notification Push (APN). Par exemple, le service APN sert à réactiver l'appareil afin qu'il puisse communiquer directement avec sa solution de GAM au moyen d'une connexion sécurisée. Aucune information confidentielle ou propriétaire n'est transmise par le service APN.

Grâce à la GAM, les services informatiques peuvent, à distance, intégrer des appareils iOS dans des environnements d'entreprise, configurer et modifier les réglages, contrôler la conformité aux règles de l'entreprise, gérer les règles de mise à jour logicielle et même verrouiller ou supprimer le contenu des appareils gérés.

Pour en savoir plus sur la GAM, rendez-vous sur :

- https://www.apple.com/ca/fr/business/resources/
- https://help.apple.com/deployment/ios/#/ior07301dd60
- https://support.apple.com/fr-ca/guide/mdm/mdmbf9e668

iPad partagé

iPad partagé est un mode multi-utilisateur que l'on peut retrouver dans les déploiements d'iPad dans un cadre éducatif. Il permet aux élèves d'utiliser un même iPad sans partager de documents ni de données. Chaque élève a son propre répertoire de départ, qui est créé en tant que volume APFS protégé par les informations d'identification de l'utilisateur. iPad partagé nécessite l'utilisation d'un identifiant Apple géré délivré et détenu par l'établissement scolaire. iPad partagé permet à un élève d'ouvrir une session sur un appareil détenu par l'établissement et configuré pour un usage par plusieurs élèves. Les données des élèves sont partitionnées en répertoires de départ distincts, chacun dans leurs propres domaines de protection des données et protégé par des autorisations UNIX et par le bac à sable.

Se connecter à iPad partagé

Lorsqu'un élève ouvre une session, l'identifiant Apple géré est authentifié par les serveurs d'identité d'Apple en faisant appel au protocole SRP. Si l'ouverture de session aboutit, un jeton d'accès éphémère, associé à l'appareil, est accordé. Si l'élève a déjà utilisé l'appareil, il dispose déjà d'un compte utilisateur local qui est alors déverrouillé avec les mêmes informations d'identification.

Si l'élève n'a jamais utilisé l'appareil, un nouvel identifiant d'utilisateur UNIX, un volume APFS qui comporte un répertoire de départ et un trousseau logique lui sont attribués. Si l'appareil n'est pas connecté à internet (car l'élève est en sortie scolaire, par exemple), l'authentification peut se faire par le compte local pour un nombre de jours limité. Dans ce cas, seuls les utilisateurs ayant déjà eu des comptes locaux peuvent se connecter. Une fois le délai expiré, les élèves doivent s'authentifier en ligne, même si un compte local existe déjà.

Après le déverrouillage ou la création du compte local de l'élève, si ce dernier s'authentifie à distance, le jeton éphémère délivré par les serveurs d'Apple est converti en jeton iCloud permettant d'ouvrir une session sur iCloud. Les réglages de l'élève sont ensuite restaurés, et ses documents et données sont synchronisés à partir d'iCloud.

Si la session de l'élève est active et que l'appareil reste en ligne, les documents et les données sont stockés sur iCloud à mesure qu'elles sont créées ou modifiées. En outre, un mécanisme de synchronisation en arrière-plan s'assure que les modifications sont envoyées à iCloud une fois que l'élève ferme sa session. 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 la saisie des informations d'identification.

Se déconnecter d'iPad partagé

Lorsqu'un élève se déconnecte d'iPad partagé, son conteneur de clés de l'utilisateur est immédiatement verrouillé et toutes les apps sont fermées. Pour accélérer la connexion d'un nouvel élève, le système reporte temporairement certaines actions de déconnexion ordinaires et affiche une fenêtre de connexion au nouvel élève. Si un élève se connecte pendant cette période (environ 30 secondes), iPad partagé effectue le nettoyage reporté dans le cadre de la connexion au compte du nouvel élève. 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 a eu lieu.

Mises à jour d'iPad partagé

Lorsqu'un iPad partagé est mis à niveau à partir d'une version antérieure à iOS 10.3 vers iOS 10.3 ou toute version ultérieure, une conversion du système de fichiers unique a lieu pour convertir la partition de données HFS+ en un volume APFS. Si à ce moment, des répertoires de départ d'utilisateurs sont présents sur le système, ils resteront sur le volume de données principal au lieu d'être convertis en volumes APFS individuels.

Lorsque d'autres élèves se connectent, leurs répertoires de départ sont également placés sur le volume de données principal. Les nouveaux comptes utilisateur ne disposeront pas de leur propre volume APFS avant que tous les comptes utilisateur du volume de données principal n'aient été supprimés. Par conséquent, pour s'assurer que les utilisateurs profitent des protections et des quotas supplémentaires fournis par APFS, l'iPad doit être mis à niveau vers la version 10.3 ou une version ultérieure au moyen d'une réinstallation complète. Sinon, tous les comptes utilisateur de l'appareil doivent être supprimés à l'aide de la commande de suppression des utilisateurs de la solution de GAM.

Pour en savoir plus sur iPad partagé, rendez-vous sur :
https://support.apple.com/fr-ca/guide/mdm/cad7e2e0cf56

Apple School Manager

Apple School Manager est un service qui s'adresse aux établissements d'enseignement et leur permet d'acheter du contenu, de configurer l'inscription automatique d'appareils dans des solutions GAM, de créer des comptes pour les élèves et le personnel, et de configurer des cours iTunes U. Apple School Manager est accessible sur le web et s'adresse aux responsables des technologies, aux administrateurs informatiques, au personnel et aux professeurs.

Pour en savoir plus sur Apple School Manager, rendez-vous sur : https://help.apple.com/schoolmanager/

Apple Business Manager

Apple Business Manager est un simple portail sur le web destiné aux administrateurs informatiques pour le déploiement d'appareils iOS, macOS et tvOS à partir du même endroit. Lorsque vous l'utilisez avec votre solution de gestion des appareils mobiles, vous pouvez configurer les réglages des appareils ainsi qu'acheter et distribuer des apps et des livres. Apple Business Manager est accessible sur le web et s'adresse aux administrateurs informatiques.

Pour en savoir plus sur Apple Business Manager, rendez-vous sur : https://help.apple.com/businessmanager/

Inscription d'appareils

Apple School Manager et Apple Business Manager offrent une façon rapide et simplifiée de déployer les appareils iOS qu'une organisation a achetés directement auprès d'Apple ou d'un fournisseur de services ou d'un revendeur agréé Apple participant. Les appareils iOS sous iOS 11 ou ultérieur et tvOS 10.2 ou ultérieur peuvent également être ajoutés à Apple School Manager et Apple Business Manager après l'achat à l'aide d'Apple Configurator 2.

Les organisations peuvent ainsi intégrer automatiquement ces appareils à leur solution de GAM sans avoir à les manipuler physiquement ni à les préparer avant de les remettre à leurs utilisateurs. Après l'inscription à un des programmes, les administrateurs se connectent au site web du programme et associent le programme à leur solution de GAM. Les appareils acquis peuvent ensuite être attribués à leurs utilisateurs au moyen de la GAM. Lors du processus de configuration de l'appareil, la sécurité des données sensibles peut être augmentée en mettant en place des mesures de sécurité appropriées. Par exemple :

- Forcez les utilisateurs à s'authentifier dans le cadre du processus de configuration initiale, et ce, par l'entremise de l'assistant réglages de l'appareil Apple, lors de l'activation.
- Proposez une configuration préliminaire à accès limité et exigez des configurations supplémentaires 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 GAM sont automatiquement installées. Toutes les transmissions entre les appareils et les serveurs d'Apple sont chiffrées au cours du transfert par HTTPS (SSL).

Il est possible de simplifier encore davantage le processus de configuration en supprimant certaines étapes dans l'assistant de configuration d'iOS, de tvOS et de macOS afin que les utilisateurs puissent être rapidement opérationnels. Les administrateurs peuvent également permettre ou non aux utilisateurs de supprimer le profil GAM de leur appareil, et s'assurer que les restrictions sur ces appareils sont en place dès le départ. Une fois déballé et activé, l'appareil est automatiquement inscrit à la solution de GAM de l'organisation, et tous les livres, applications et réglages de gestion sont installés.

Apple Configurator 2

Outre le système de GAM, Apple Configurator 2 pour macOS simplifie la configuration des appareils iOS et des Apple TV avant leur distribution aux utilisateurs. Grâce à Apple Configurator 2, les apps, les données, les restrictions et les réglages des appareils peuvent être rapidement configurés.

Apple Configurator 2 permet d'utiliser Apple School Manager ou Apple Business Manager pour inscrire les appareils à une solution de GAM sans utiliser l'assistant de configuration. Apple Configurator 2 peut également être utilisé pour ajouter des appareils iOS et des Apple TV à Apple School Manager ou Apple Business Manager après leur achat.

Pour obtenir plus d'informations sur Apple Configurator 2, rendez-vous sur : https://support.apple.com/fr-ca/guide/apple-configurator-2/

Supervision

Pendant la configuration d'un appareil, une entreprise peut configurer ce dernier de façon à ce qu'il soit supervisé. La supervision indique qu'un organisme détient l'appareil dans le but d'assurer un contrôle supplémentaire sur sa configuration et ses restrictions. Avec Apple School Manager ou Apple Business Manager, la supervision peut être activée sans fil sur l'appareil dans le cadre du processus d'inscription à la GAM ou manuellement à l'aide d'Apple Configurator 2. Pour qu'un appareil soit supervisé, celui-ci doit être effacé, et son système d'exploitation réinstallé.

Pour en savoir plus sur la configuration et la gestion d'appareils iOS et d'Apple TV à l'aide d'une solution de GAM ou d'Apple Configurator 2, rendez-vous sur : https://help.apple.com/deployment/ios/

Restrictions

Des restrictions peuvent être activées ou, dans certains cas, désactivées par les administrateurs afin d'empêcher les utilisateurs d'accéder à une app, à un service ou à une fonction de l'appareil. Les restrictions sont envoyées aux appareils dans une entité de restrictions jointe à un profil de configuration. Les restrictions peuvent être appliquées aux appareils iOS, tvOS et macOS. Parmi les restrictions d'un iPhone géré, certaines peuvent être mises en miroir sur une Apple Watch jumelée.

Pour voir la liste actualisée destinée aux gestionnaires informatiques, rendez-vous sur : https://support.apple.com/fr-ca/guide/mdm/mdm0f7dd3d8

Effacement à distance

Les appareils iOS peuvent être effacés à distance par un administrateur ou un utilisateur. L'effacement instantané à distance est effectué en éliminant de manière sécurisée la clé de chiffrement de stockage en blocs du stockage effaçable, ce qui rend toutes les données illisibles. La commande d'effacement à distance peut être envoyée à partir de la GAM, d'Exchange ou d'iCloud.

Lorsqu'une commande d'effacement à distance est déclenchée au moyen de la GAM ou d'iCloud, l'appareil envoie une confirmation et effectue l'effacement des données. Pour l'effacement à distance par Exchange, l'appareil confirme la commande auprès du serveur Exchange avant d'effectuer l'effacement des données.

Les utilisateurs ont également la possibilité d'effacer le contenu des appareils en leur possession en utilisant l'app Réglages. Enfin, comme mentionné précédemment, il est possible de régler les appareils afin qu'ils effacent automatiquement leurs données après un certain nombre de tentatives manquées de saisie de code.

Mode Perdu

Si un appareil est perdu ou volé, un administrateur de GAM peut activer à distance le mode Perdu sur un appareil supervisé doté d'iOS 9.3 ou version ultérieure. Lorsque le mode Perdu est activé, l'utilisateur actif est déconnecté et l'appareil ne peut pas être déverrouillé. L'écran affiche un message que l'administrateur peut personnaliser, par exemple un numéro de téléphone à appeler si l'appareil est retrouvé. Quand l'appareil est placé en mode Perdu, l'administrateur peut demander à l'appareil d'envoyer sa position et, facultativement, d'émettre un son. Si un administrateur désactive le mode Perdu, ce qui constitue le seul moyen de quitter le mode, l'utilisateur est informé de cette opération par un message sur l'écran verrouillé ou une alerte sur l'écran d'accueil.

Verrouillage d'activation

Lorsque la fonctionnalité Localiser mon iPhone est activée, il est impossible de réactiver un appareil sans saisir l'identifiant Apple et le mot de passe du propriétaire ou le code antérieur de l'appareil.

Pour les appareils détenus par une organisation, il peut s'avérer judicieux de les superviser de sorte que la fonction de verrouillage d'activation puisse être gérée par l'organisation plutôt que de demander à chaque utilisateur de saisir ses informations d'identification Apple pour réactiver son appareil.

Sur des appareils supervisés, une solution de GAM compatible peut ensuite conserver un code de contournement lorsque le verrouillage d'activation est activé et utiliser ce code ultérieurement pour retirer automatiquement le verrouillage d'activation lorsqu'un appareil doit être effacé et attribué à un nouvel utilisateur.

Par défaut, le verrouillage d'activation n'est jamais possible sur des appareils supervisés, même si l'utilisateur active la fonctionnalité Localiser mon iPhone. Un serveur de GAM peut toutefois récupérer un code de contournement et autoriser l'activation du verrouillage d'activation sur l'appareil. Si la fonctionnalité Localiser mon iPhone est activée lorsque la solution de GAM autorise le verrouillage d'activation, le verrouillage est

activé à partir de ce moment. Si la fonctionnalité Localiser mon iPhone est désactivée lorsque le serveur de GAM autorise le verrouillage d'activation, ce dernier est activé dès que l'utilisateur en fait de même pour Localiser mon iPhone.

Pour les appareils utilisés en milieu scolaire avec un identifiant Apple géré créé dans Apple School Manager, la fonction de verrouillage d'activation peut être liée à l'identifiant Apple d'un administrateur plutôt qu'à celui des utilisateurs, ou être désactivée à l'aide du code de contournement de l'appareil.

Temps d'écran

Temps d'écran est une fonctionnalité d'iOS 12 qui permet à un utilisateur de comprendre et de contrôler sa propre utilisation d'apps et du web ainsi que celle de ses enfants. Les utilisateurs peuvent :

- visionner les données sur l'utilisation;
- régler les limites d'utilisation des apps et du web;
- configurer Temps d'arrêt;
- faire respecter des restrictions supplémentaires.

Pour un utilisateur qui gère sa propre utilisation de l'appareil, les données sur l'utilisation et les contrôles de Temps d'écran peuvent être synchronisés entre les appareils associés au même compte iCloud à 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 désactivée par défaut). Temps d'écran remplace la fonctionnalité Restrictions des versions antérieures d'iOS.

Lorsqu'un utilisateur vide son historique Safari ou qu'il supprime une application, 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 pour comprendre 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 surveiller leur propre utilisation. Lorsque les parents activent Temps d'écran pour leurs enfants, ils règlent un code pour empêcher à leurs enfants d'apporter des modifications. À l'âge de 18 ans (selon le pays ou la région), les enfants peuvent désactiver cette surveillance.

Les données sur l'utilisation et les réglages de configuration sont transférés entre les appareils du parent et de l'enfant à l'aide d'une connexion à l'IDS chiffrée 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 ou l'iPad 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 pendant l’assistant de configuration ou plus tard dans Réglages;
- 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’apps.

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.

Contrôles de confidentialité

Apple accorde une grande importance à la protection des données personnelles de ses clients et a conçu plusieurs options et commandes intégrées qui permettent aux utilisateurs iOS de déterminer la manière dont les applications utilisent leurs informations, le moment où elles le font et la nature des informations utilisées.

Service de localisation

Le service de localisation utilise les données GPS, la connexion Bluetooth et une base de données communautaire des emplacements des bornes d'accès Wi-Fi et des antennes-relais de téléphonie cellulaire pour déterminer la position approximative des utilisateurs. Le service de localisation peut être désactivé au moyen d'un commutateur unique dans Réglages. L'utilisateur a également la possibilité d'autoriser l'accès de chaque app à ce service. Chaque app peut demander l'autorisation de recevoir des données de localisation de manière permanente ou uniquement lorsqu'elle est utilisée. L'utilisateur peut décider de ne pas autoriser cet accès et peut modifier son choix à tout moment dans Réglages. Dans Réglages, l'utilisateur peut choisir de ne jamais autoriser l'accès, de l'autoriser ponctuellement en cas d'utilisation ou de l'autoriser en permanence, en fonction de l'usage de la localisation demandée par l'app. Par ailleurs, si une app autorisée à utiliser les données de localisation en permanence profite de cette autorisation alors qu'elle est exécutée en arrière-plan, un message est envoyé à l'utilisateur pour le prévenir et lui donner la possibilité de modifier l'autorisation d'accès de l'app.

L'utilisateur dispose en outre d'un contrôle précis sur la manière dont les services du système utilisent les données de localisation. Cette fonctionnalité permet de désactiver l'inclusion des données de localisation dans les informations recueillies par les services d'analyse employés par Apple pour améliorer iOS, les informations de Siri selon le lieu, le contexte basé selon le lieu des suggestions de Siri, les conditions de circulation locales et les lieux importants visités précédemment.

Accès aux données personnelles

iOS aide à interdire l'accès non autorisé des apps aux données personnelles de l'utilisateur. Ce dernier peut en plus utiliser Réglages pour voir quelles sont les apps autorisées à accéder à certaines informations et pour accorder ou refuser toute autorisation d'accès ultérieure. Cela comprend l'accès aux éléments suivants :

- Contacts
- Calendriers
- Rappels
- Photos
- Activité et forme physique
- Service de localisation
- Apple Music
- L'activité liée à votre musique ou à vos vidéos
- Micro
- Caméra
- HomeKit
- Santé
- Reconnaissance vocale
- Partage Bluetooth
- Votre bibliothèque multimédia

Si l'utilisateur se connecte à iCloud, les apps sont autorisées par défaut à se connecter à iCloud Drive. L'utilisateur peut contrôler l'accès de chaque app sous iCloud (Réglages > Nom de l'utilisateur). iOS fournit également des restrictions qui interdisent tout mouvement de données entre les apps et les comptes installés par une solution de GAM et ceux installés par l'utilisateur.

Politique de confidentialité

Pour lire la politique de confidentialité d'Apple, rendez-vous sur : https://www.apple.com/ca/fr/legal/privacy

Certificats et programmes de sécurité

Remarque : pour obtenir les informations les plus récentes sur les certifications de sécurité, les procédures de validation et les instructions relatives à iOS, rendez-vous sur : https://support.apple.com/HT202739

Certifications ISO 27001 et 27018

Apple a obtenu les certifications ISO 27001 et 27018 pour le système de gestion de sécurité des informations pour l'infrastructure, le développement et les opérations qui prennent en charge ces produits et services : Apple School Manager, iTunes U, iCloud, iMessage, FaceTime, identifiants Apple gérés, Siri, et Pour l'école, conformément à la Déclaration d'applicabilité (Statement of Applicability) v2.1 du 11 juillet 2017. La conformité d'Apple aux normes ISO a été certifiée par le British Standards Institution (BSI). Les certificats de conformité ISO 27001 et ISO 27018 se trouvent sur le site web du BSI. Pour consulter ces certificats, rendez-vous sur :

https://www.bsigroup.com/fr-CA/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=apple&licencenumber=IS+649475

https://www.bsigroup.com/fr-CA/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=Apple&licencenumber=PII%20673269

Validation cryptographique (FIPS 140-2)

La conformité des modules de chiffrement d'iOS a été validée à plusieurs reprises selon la norme FIPS (Federal Information Processing Standards) 140-2 des États-Unis à chaque nouvelle version depuis iOS 6. Comme c'est le cas pour chaque version majeure, Apple soumet les modules au CMVP pour qu'ils soient revalidés lors de la sortie de la nouvelle version du système d'exploitation iOS. Ce programme confirme l'intégrité des opérations de chiffrement pour les apps d'Apple et les apps tierces qui exploitent correctement les services cryptographiques d'iOS ainsi que les algorithmes approuvés.

Apple a reçu la validation FIPS 140-2 pour le module matériel intégré connu sous le nom de **module cryptographique du trousseau de clés sécurisées (SKS) du processeur Secure Enclave (SEP)** qui permet l'utilisation approuvée des clés générées et gérées par le SEP. Apple continuera de tenter d'atteindre des niveaux supérieurs pour le module matériel avec chaque version ultérieure majeure d'iOS au besoin.

Certification des critères communs (ISO 15408)

Depuis le lancement d'iOS 9, Apple a obtenu des certifications ISO pour chaque version majeure dans le cadre du programme de certification des critères communs et a étendu sa couverture pour inclure ce qui suit :

- le profil de protection fondamentale des appareils mobiles;
  - le module étendu pour les agents de gestion des appareils mobiles;
  - le module étendu pour les clients réseau sans fil;
  - le module PP pour le client VPN;
- le profil de protection pour le logiciel d'application;
  - le module étendu pour les navigateurs web.
- Apple compte étendre la couverture pour chaque version ultérieure majeure d'iOS.

Apple joue un rôle actif au sein de la communauté technique internationale (ITC) dans le développement de profils de protection collaboratifs (cPP) actuellement indisponibles axés sur l'évaluation des technologies de sécurité mobile des clés. Apple poursuit ses efforts pour examiner et obtenir de nouvelles certifications relatives aux nouvelles versions actualisées des cPP disponibles à ce jour et en développement.

Solutions commerciales pour composants classifiés (CSfC)

Le cas échéant, Apple a également soumis la plateforme iOS et différents services pour les inclure dans la liste des composants du programme des solutions commerciales pour composants classifiés (CSfC). Dans la mesure où les plateformes et les services Apple font l'objet de certifications inhérentes aux critères communs, ils seront également soumis à leur ajout dans la liste des composants du programme CSfC.

Pour connaître les composants les plus récemment répertoriés, rendez-vous sur : https://www.nsa.gov/resources/everyone/csfc/components-list/

Guides de configuration de sécurité

Apple a collaboré avec les gouvernements du monde entier pour mettre au point des guides donnant les instructions et recommandations nécessaires pour le maintien d'un environnement plus sécurisé, également appelé « durcissement des appareils pour les environnements à haut risque ». Ces guides fournissent des informations bien définies et approfondies sur la configuration et l'utilisation de fonctionnalités intégrées d'iOS pour une protection améliorée.

Prime de sécurité d’Apple

Apple récompense les chercheurs qui partagent des problèmes critiques avec Apple. Pour être admissibles à la prime de sécurité d’Apple, les chercheurs doivent fournir un rapport et une démonstration de faisabilité clairs. La vulnérabilité doit porter atteinte à la dernière version d’iOS et, le cas échéant, à l’appareil le plus récent. Apple effectuera une évaluation pour déterminer le montant exact de la prime, qui peut varier, entre autres, selon l’ordre des signalements, la nouveauté, la probabilité d’exposition et le niveau d’interaction requis.

Dès que les problèmes lui sont correctement communiqués, Apple s’engage à résoudre aussi vite que possible ceux qui sont confirmés. Le cas échéant et sauf demande contraire, la découverte d’une vulnérabilité fera l’objet d’une reconnaissance publique par Apple.

Catégorie	Paiement maximum (USD)
Composants du programme interne de démarrage sécurisé	200 000 $
Extraction de données personnelles protégées par le Secure Enclave	100 000 $
Exécution de code arbitraire avec privilèges de noyau	50 000 $
Accès non autorisé aux données de compte iCloud sur les serveurs Apple	50 000 $
Accès, à partir d’un processus en bac à sable, à des données d’utilisateur en dehors de cet environnement cloisonné	25 000 $

Si la prime est donnée à un organisme de bienfaisance admissible, Apple fera une contribution équivalente.

Pour en savoir plus sur le signalement des bogues à Apple, rendez-vous sur : https://developer.apple.com/bug-reporting/

Conclusion

Un engagement en faveur de la sécurité

Apple s'engage à contribuer à la protection de ses clients en leur proposant des technologies avancées de sécurité et de confidentialité conçues pour protéger leurs données personnelles, ainsi que des méthodes complètes destinées à protéger les données professionnelles dans les environnements d'entreprise.

La sécurité fait partie intégrante du système iOS. De la plateforme au réseau, en passant par les apps, iOS possède tout ce dont une entreprise a besoin. Ensemble, ces composants confèrent à iOS les fonctionnalités de sécurité les plus performantes du marché, sans compromettre l'expérience d'utilisation.

Apple fait appel à une infrastructure de sécurité intégrée et cohérente à travers tout le système iOS et l'écosystème constitué par les apps iOS. Le chiffrement matériel des espaces de stockage fournit des capacités d'effacement à distance en cas de perte d'appareil et permet aux utilisateurs de supprimer complètement toutes leurs données personnelles ainsi que celles de l'entreprise en cas de revente de leur appareil ou de son transfert à une autre personne. Les informations utilisées pour le diagnostic sont également collectées de manière anonyme.

Les apps iOS conçues par Apple sont développées dans un souci de sécurité avancée. Par exemple, iMessage et FaceTime fournissent un chiffrement client-à-client. Pour les apps tierces, la combinaison de la signature obligatoire du code, du cloisonnement des applications et des déclarations d'autorisation fournit aux utilisateurs une protection de pointe contre les virus, les logiciels malveillants et d'autres programmes. Le processus de soumission à l'App Store renforce la protection des utilisateurs contre ces risques, car chaque app iOS est examinée avant d'être mise sur le marché.

Pour tirer le meilleur parti des fonctionnalités de sécurité étendues intégrées dans iOS, les entreprises sont encouragées à revoir leurs politiques en matière de sécurité et de services informatiques afin de s'assurer qu'elles exploitent au mieux les couches de technologies de sécurité offertes par cette plateforme.

Apple dispose d'une équipe de sécurité spécialisée, chargée de fournir une assistance pour tous les produits Apple. L'équipe propose des services d'audit et de test aussi bien pour les produits en développement que pour les produits déjà commercialisés. L'équipe Apple fournit également des formations et des outils de sécurité et se tient activement informée de tous les rapports concernant les nouveaux problèmes et menaces de sécurité. Apple fait partie du forum FIRST (Forum of Incident Response and Security Teams) qui rassemble des équipes chargées de la sécurité et de la réponse aux incidents.

Pour en savoir plus sur le signalement de problèmes à Apple et l'abonnement aux notifications de sécurité, rendez-vous sur : https://www.apple.com/ca/fr/support/security

Glossaire

APN (Apple Push Notification), service de notification Push d'Apple	Service mondial offert par Apple pour fournir des notifications de type Push aux appareils iOS.
bits logiciels de départ	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 logiciel de départ 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 logiciels de départ pourvu que le bit de verrouillage correspondant n'ait pas été réglé. Une fois le bit de verrouillage réglé, ce dernier et le bit logiciel de départ ne peuvent plus être modifiés. Les bits logiciels de départ et leur bit de verrouillage sont réinitialisés quand le Secure Enclave redémarre.
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.
circuit intégré (CI)	Également appelé micropuce.
clé de fichier	Clé AES 256 bits utilisée pour chiffrer un fichier du système de fichiers. La clé de fichier est enveloppée par une clé de classe et stockée dans les métadonnées du fichier.
clé du système de fichiers	Clé permettant de chiffrer les métadonnées de chaque fichier, y compris la clé de classe. Elle est conservée dans l'espace de stockage effaçable pour permettre l'effacement à distance plutôt que pour des raisons de confidentialité.
conteneur de clés	Structure de données utilisée pour stocker une collection de clés de classe. Chaque type (utilisateur, appareil, système, sauvegarde, dépôt ou Sauvegarde iCloud) possède le même format : • Un en-tête contenant : – la version (réglée sur 3 dans iOS 5); – le type (système, sauvegarde, dépôt 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 : emmêlées avec l'UID ou PBKDF2, ainsi que le salage et le nombre d'itérations. • Une liste de clés de classe : – UUID de clé; – classe (classe de protection des données de trousseau ou de fichier); – Type d'encapsulation (clé dérivée de l'UID uniquement; clé dérivée de l'UID et clé dérivée du code); – clé de classe enveloppée; – clé publique pour classes asymétriques.
contrôleur de mémoire	Sous-système de la puce-système qui contrôle l'interface entre la puce-système et sa mémoire principale.
DFU (Device Firmware Upgrade), mise à niveau de logiciel interne d'appareil	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 : « iTunes a détecté un iPad en mode de récupération. Vous devez restaurer cet iPad avant de pouvoir l'utiliser avec iTunes. »
ECDSA	Un algorithme de signature numérique fondé sur la cryptographie à courbe elliptique.
échange Diffie-Hellman à courbe elliptique (ECDHE)	Échange Diffie-Hellman à courbe elliptique avec clés éphémères. 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. Grâce à cette technique, 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 PRF pour chaque itération.
enveloppement de clé	Chiffrement d'une clé à l'aide d'une autre clé. iOS utilise l'enveloppement de clé NIST AES conforme à la norme RFC 3394.
iBoot	Code qui charge XNU, dans le cadre d'une chaîne de démarrage sécurisée. Selon la génération de la puce-système, iBoot pourrait être chargé par LLB ou 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 puce exclusif (ECID)	Identifiant 64 bits propre au processeur de chaque appareil iOS. Si un appel est pris sur un appareil, la sonnerie sur les appareils à proximité et jumelés via iCloud est coupée par le biais d'une brève notification Bluetooth Low Energy 4.0. Les octets de cette notification sont chiffrés par la même méthode que les notifications de type Handoff. Il 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.
LLB (Low-Level Bootloader), chargeur d'amorçage de niveau inférieur	Sur les systèmes dotés d'une architecture de démarrage à deux étape, code invoqué par la mémoire morte d'amorçage, qui charge à son tour l'iBoot dans le cadre d'une chaîne de démarrage sécurisée.
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 attaquant.
mode de récupération	Le mode de récupération est utilisé pour restaurer un appareil iOS ou une Apple TV si : • iTunes ne reconnaît pas votre appareil ou indique qu'il est en mode de récupération; • l'écran affiche le logo Apple pendant plusieurs minutes sans barre de progression; • l'écran de connexion à iTunes apparaît.
module de sécurité matériel (HSM)	Ordinateur spécialisé, protégé contre toute manipulation, utilisé pour sauvegarder et gérer des clés numériques.
profil d'approvisionnement	Fichier plist signé 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. Un profil d'approvisionnement de développement répertorie les appareils sélectionnés par un développeur en vue d'une distribution ad hoc. Un profil d'approvisionnement de distribution contient l'identifiant d'une app développée par une entreprise.
protection de données	Mécanisme de protection des fichiers et des trousseaux pour iOS. Cette expression peut également faire référence aux API utilisées par des apps pour protéger des fichiers et des éléments de trousseau.
protection de l'intégrité du coprocesseur système (SCIP)	Les coprocesseurs système sont des processeurs situés sur la même puce-système que le processeur d'application.
protocole de distribution aléatoire de l'espace d'adressage (ASLR)	Technique utilisée par iOS 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. Sous iOS 5 ou version ultérieure, la position de toutes les bibliothèques et apps système est déterminée de manière aléatoire, de même que celle des apps de tiers compilées en tant qu'exécutables indépendants de la position.
puce-système	Circuit intégré (CI) incorporant plusieurs composants sur une seule puce. Le processeur d'application, le Secure Enclave et les autres coprocesseurs sont des composants de la puce-système.

registre de progression du démarrage (BPR)	Un ensemble de drapeaux matériels de puces-systèmes qu'un logiciel peut utiliser pour faire le suivi des modes de démarrage que l'appareil a déclenchés, comme le mode DFU ou le mode de récupération. Une fois un drapeau du registre de progression du démarrage réglé, il ne peut pas être effacé. Il permet aux logiciels ultérieurs d'obtenir un indicateur de confiance de l'état du système.
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.
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 l'attaquant prend physiquement possession de l'appareil, les clés conservées dans l'espace de stockage effaçable peuvent être utilisées dans le cadre d'une hiérarchie de clés pour faciliter l'effacement à distance et renforcer la sécurité.
trousseau	L'infrastructure et un ensemble d'API utilisés par iOS et les apps de tiers pour stocker et récupérer des mots de passe, des clés et d'autres informations d'identification délicates.
UID (Unique ID), identifiant unique	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 attaquant potentiel devrait lancer une attaque physique onéreuse et extrêmement sophistiquée contre le silicium du processeur. L'UID n'est lié à aucun autre identifiant présent sur l'appareil, tel que l'UDID par exemple.
URI (Uniform Resource Identifier), identifiant de ressource uniforme	Chaîne de caractères permettant d'identifier une ressource web.
XNU	Noyau au centre des systèmes d'exploitation iOS et macOS. Il est supposé fiable et permet d'appliquer des mesures de sécurité telles que la signature de code, la mise en bac à sable des applications (sandboxing), la vérification des déclarations d'autorisation et la distribution aléatoire de l'espace d'adressage (ASLR).

Historique des révisions du document

Date	Résumé
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
Septembre 2018	**Actualisé pour iOS 12** • Secure Enclave • Protection de l'intégrité du système d'exploitation • Carte Express avec réserve d'énergie • 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 d'entreprise • Messages dans iCloud • Apple Business Manager
Décembre 2017	**Actualisé pour iOS 11.2** • Apple Pay Cash **Actualisé pour iOS 11.1** • Certificats et programmes de sécurité • Touch ID et Face ID • Notes partagées • Chiffrement de bout en bout CloudKit • TLS • Apple Pay, utilisation d'Apple Pay pour effectuer des paiements en ligne • Suggestions de Siri • iPad partagé

Date	Résumé
Juillet 2017	**Actualisé pour iOS 10.3** • System Enclave • Protection des données des fichiers • Conteneurs de clés • Certificats et programmes de sécurité • SiriKit • HealthKit • Sécurité du réseau • Bluetooth • iPad partagé • Mode Perdu • Verrouillage d'activation • Contrôles de confidentialité
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 pour effectuer des paiements en ligne • Approvisionnement 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

Date	Résumé
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 • Sécurité du transport des apps • Spécifications VPN • Accès distant à iCloud pour HomeKit • Cartes de fidélité Apple Pay, app de l'émetteur de carte Apple Pay • Indexation Spotlight sur l'appareil • Modèle de jumelage iOS • Apple Configurator 2 • Restrictions

Mai 2019