Sécurité iOS

iOS 12.1

Novembre 2018

Table des matières

Page 5 **Introduction**

Page 7 **Sécurité du système**
Chaîne de démarrage sécurisé
Autorisation du logiciel système
Secure Enclave
Protection de l’intégrité du système d’exploitation
Touch ID
Face ID

Page 17 **Chiffrement et protection des données**
Fonctionnalités de sécurité du matériel
Protection des données des fichiers
Codes de verrouillage
Classes de protection des données
Protection des données du trousseau
Conteneurs de clés

Page 29 **Sécurité des apps**
Signature du code des apps
Sécurité des processus exécutés
Extensions
Groupes d’apps
Protection des données dans les apps
Accessoires
HomeKit
SiriKit
HealthKit
ReplayKit
Notes sécurisées
Notes partagées
Apple Watch

Page 45 **Sécurité du réseau**
TLS
VPN
Wi-Fi
Bluetooth
Authentification unique
Continuité
Sécurité AirDrop
Partage du mot de passe Wi-Fi

Page 54 **Apple Pay**
Composants d'Apple Pay
Comment Apple Pay utilise Secure Element
Comment Apple Pay utilise le contrôleur NFC
Transfert sur cartes bancaires et prépayées
Autorisation du paiement
Code de sécurité dynamique propre à la transaction
Paiement à l'aide de cartes bancaires dans les magasins
Paiement à l'aide de cartes bancaires dans les apps
Paiement à l'aide de cartes bancaires sur le web
Cartes sans contact
Apple Pay Cash
Cartes de transport
Cartes d'étudiant
Suspension, retrait et effacement de cartes

Page 67 **Services Internet**
Identifiant Apple
iMessage
Business Chat
FaceTime
iCloud
Trousseau iCloud
Siri
Suggestions Safari, Suggestions Siri dans les recherches, Recherche, #images, app News et widget News dans les pays sans l'app News
Prévention intelligente du suivi dans Safari

Page 86 **Gestion des mots de passe d'utilisateur**
Accès des apps aux mots de passe enregistrés
Mots de passe complexes automatiques
Envoi de mots de passe à d'autres personnes ou appareils
Extensions de fournisseur d'informations d'identification

Page 89 **Contrôle des appareils**
Protection par code de verrouillage
Modèle de jumelage iOS
Application de la configuration
Mobile Device Management - Gestion des appareils mobiles (MDM)
iPad partagé
Apple School Manager
Apple Business Manager
Enregistrement d'appareils
Apple Configurator 2
Supervision
Restrictions
Effacement à distance
Mode Perdu
Verrouillage d'activation
Temps d'écran

Page 99 **Contrôles de confidentialité**
Service de localisation
Accès aux données personnelles
Politique de confidentialité

Page 101 **Certificats et programmes de sécurité**
Certifications ISO 27001 et 27018
Validation cryptographique (FIPS 140-2)
Certification des critères communs (ISO 15408)
Solutions commerciales pour composants classifiés (CSfC)
Guides de configuration de sécurité

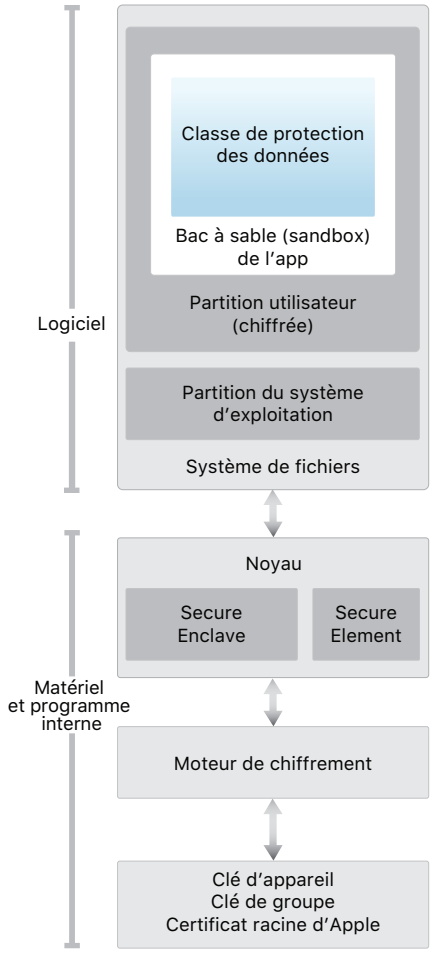
Page 103 **Récompense de sécurité Apple**

Page 104 **Conclusion**
Un engagement en faveur de la sécurité

Page 105 **Glossaire**

Page 108 **Historique des révisions du document**

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 dans 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 termes 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 par l'utilisateur. 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 l'implémentation 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, l'iPad et 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 standards de mise en réseau qui assurent la sécurisation de l'authentification et le chiffrement des données lors des transmissions.
- **Apple Pay :** l'implémentation 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 par mot de passe et accès à des mots de passe provenant 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 :** information sur les certifications ISO, validation cryptographique, certification des critères communs et solutions commerciales pour composants classifiés (CSfC).

Sécurité du système

Accès au mode de mise à niveau du logiciel interne d'un appareil (DFU)

La restauration d'un appareil placé en mode DFU (également connu sous le nom de mode de récupération) permet de revenir à un état de bon fonctionnement connu de cet appareil en ayant la certitude qu'il ne contient que du code intact signé par Apple. Le mode DFU est accessible manuellement.

Connectez tout d'abord l'appareil à un ordinateur en utilisant un câble USB.

Effectuez ensuite l'une des opérations suivantes en fonction de votre appareil :

iPhone X ou ultérieur, iPhone 8 ou iPhone 8 Plus. Appuyez brièvement sur le bouton d'augmentation du volume. Appuyez brièvement sur le bouton de diminution du volume. Maintenez le bouton latéral enfoncé et appuyez de nouveau sur le bouton de diminution du volume. Relâchez le bouton latéral après cinq secondes, puis maintenez le bouton de diminution du volume appuyé jusqu'à ce que vous accédiez à l'écran du mode de récupération.

iPhone 7 ou iPhone 7 Plus. Appuyez simultanément sur le bouton latéral et sur le bouton de diminution du volume et maintenez-les enfoncés. Relâchez le bouton latéral et maintenez le bouton de diminution du volume appuyé jusqu'à ce que vous accédiez à l'écran du mode de récupération.

La sécurité du système est conçue de sorte que le logiciel et le matériel soient sécurisés dans tous les composants clés de chaque appareil iOS. Cela inclut le processus de démarrage, les mises à jour du logiciel et 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 services et des technologies logicielles et matérielles 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 sécurisé

Chaque étape du processus de démarrage contient des composants qui sont signés cryptographiquement par Apple pour garantir leur intégrité et qui ne s'exécutent qu'une fois la chaîne de confiance vérifiée. Cela concerne notamment les chargeurs de démarrage, le noyau, les extensions du noyau et le programme interne de bande de base. Cette chaîne de démarrage sécurisé permet de s'assurer que les niveaux les plus bas du logiciel 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 **ROM de démarrage**. 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 ROM de démarrage contient la clé publique de l'autorité de certificat racine d'Apple, qui est utilisée pour vérifier que le chargeur de démarrage 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. Une fois les tâches d'iBoot terminées, le chargeur vérifie et exécute le noyau iOS. Pour les appareils dotés d'un processeur A9 ou antérieur de la série A, une phase supplémentaire du **chargeur de démarrage de bas niveau (LLB)** est incluse et vérifiée au chargement par la ROM de démarrage, laquelle charge et vérifie à son tour iBoot.

Toute incapacité de la ROM de démarrage à charger le LLB (sur les anciens appareils) ou iBoot (sur les appareils plus récents) se traduit par l'entrée de l'appareil en mode DFU. En cas d'incapacité du LLB ou d'iBoot à charger et vérifier l'étape suivante, le démarrage est interrompu et l'appareil affiche l'écran de connexion à iTunes. C'est ce que l'on appelle le mode de récupération. Quel que soit le cas de figure, l'appareil doit être connecté à iTunes par USB pour rétablir ses réglages par défaut d'origine.

iPhone 6s et modèles précédents, iPad ou iPod touch. Maintenez le bouton principal et le bouton supérieur (ou latéral) simultanément enfoncés. Relâchez le bouton supérieur (ou latéral) et maintenez le bouton du menu principal appuyé jusqu'à ce que vous accédiez à l'écran du mode de récupération.

Remarque : rien ne s'affiche à l'écran lorsque l'appareil est en mode DFU. Si le logo Apple apparaît, cela signifie que vous avez appuyé trop longtemps sur le bouton latéral ou le bouton Marche/Veille.

Le **registre de progression du démarrage (Boot Progress Register, ou BPR)** est utilisé par le Secure Enclave pour limiter l'accès aux données d'utilisateur dans différents modes et est actualisé avant d'accéder aux modes suivants :

- **Mode de récupération :** défini par iBoot sur les appareils équipés de **systèmes sur puce (SoC)** Apple A10, S2 ou de modèles plus récents.
- **Mode DFU :** défini par la ROM de démarrage sur les appareils équipés d'un système sur puce A12.

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

Sur les appareils avec accès mobile, le sous-système de bande de base fait également appel à un processus de démarrage sécurisé similaire, avec du code logiciel signé et des clés vérifiées 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 » de ce document.

Pour en savoir plus sur le passage manuel en mode de récupération, consultez l'article : https://support.apple.com/HT1808

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 d'un Secure Enclave, le coprocesseur Secure Enclave s'appuie également sur 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 » de ce document.

Les mises à jour du logiciel iOS peuvent être installées sur l'appareil en utilisant iTunes ou la technologie sans fil Over-The-Air (OTA). Avec iTunes, une copie complète d'iOS est téléchargée et installée. Les mises à jour du logiciel en mode OTA 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. Par ailleurs, les mises à jour de logiciels peuvent être mises en cache sur un Mac exécutant macOS High Sierra avec la fonction Mise en cache du contenu activée, de telle sorte que les appareils iOS n'ont pas besoin de télécharger à nouveau la mise à jour nécessaire via Internet. Ils ont alors tout de même besoin de contacter les serveurs Apple pour mener à bien la procédure 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 du logiciel en mode OTA) se connecte au serveur d'autorisation d'installation d'Apple et lui envoie une liste de mesures cryptographiques pour chaque partie du paquet à installer (par exemple, iBoot, le noyau et l'image du système d'exploitation), une valeur anti-répétition aléatoire (nonce) et l'**identifiant unique de l'appareil (ECID)**.

Le serveur d'autorisation compare alors la liste de mesures qui lui est fournie et les 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 depuis le disque, associée à l'ECID de l'appareil, correspond à ce que couvre la signature. Ces étapes permettent de s'assurer que l'autorisation est destinée à un appareil spécifique et qu'il est impossible de copier une ancienne version d'iOS d'un appareil à l'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

Secure Enclave est un coprocesseur fabriqué au sein du système sur puce (SoC). Il utilise une mémoire chiffrée et intègre un générateur de nombres aléatoires matériel. Secure Enclave assure toutes les opérations cryptographiques pour la gestion des clés de **protection des données** et préserve l'intégrité de la protection des données même si le noyau a été compromis. La communication entre Secure Enclave et le processeur d'application se limite à une boîte aux lettres déclenchée par interruption et à des tampons de données de mémoire partagée.

Secure Enclave comprend une ROM de démarrage Secure Enclave dédiée. Semblable à la ROM de démarrage du processeur d'application, la ROM de démarrage Secure Enclave est un code immuable qui établit la racine matérielle de confiance du coprocesseur Secure Enclave.

Secure Enclave exécute un système d'exploitation Secure Enclave basé sur une version adaptée par Apple du micronoyau L4. Le système d'exploitation Secure Enclave est signé par Apple, vérifié par la ROM de démarrage Secure Enclave et actualisé au moyen d'un processus de mise à jour logicielle personnalisé.

Au démarrage de l'appareil, une clé éphémère de protection de mémoire est créée par la ROM de démarrage Secure Enclave, combinée à l'UID de l'appareil et utilisée pour chiffrer la partie de l'espace mémoire de l'appareil réservée à Secure Enclave. Sauf sur l'Apple A7, la mémoire Secure Enclave est également authentifiée à l'aide de la clé de protection de mémoire. Sur les SoC A11 et S4 plus récente, ainsi que les modèles plus récents, une arborescence d'intégrité est utilisée pour empêcher la répétition de la mémoire Secure Enclave essentielle pour la sécurité, authentifiée par la clé de protection de mémoire et les nonces stockés en mémoire SRAM embarquée sur le processeur.

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 à un compteur anti-répétition. Le compteur anti-répétition est stocké dans un **circuit intégré (CI)** dédié à la mémoire non volatile.

Sur les appareils équipés de SoC A12 et S4, le Secure Enclave est associé à un circuit intégré de stockage sécurisé (CI) destiné à stocker le compteur anti-répétition. Le CI de stockage sécurisé est constitué d'un code de ROM immuable, d'un générateur matériel de nombres aléatoires, de moteurs cryptographiques et d'un détecteur de manipulation physique. Pour lire les compteurs et les mettre à jour, le Secure Enclave et le CI de stockage utilisent un protocole sécurisé qui garantit un accès exclusif aux compteurs.

Les services anti-répétition du Secure Enclave sont utilisés pour la révocation des données sur des événements qui marquent les limites de l'anti-répétition, notamment ce qui suit :

- modification du code ;
- activation/désactivation de Touch ID ou Face ID ;
- ajout/suppression des empreintes ;
- réinitialisation de Face ID ;
- ajout/retrait de carte Apple Pay ;
- effacer contenu et réglages.

Le Secure Enclave permet également de traiter les empreintes et les données faciales générées par les capteurs Touch ID et Face ID pour déterminer s'il existe une correspondance avant d'autoriser l'accès ou l'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 effectuée, le système de protection de l'intégrité du noyau (KIP) est activé pour éviter toute modification du noyau et de ses gestionnaires. Le **contrôleur de mémoire** fournit une région de mémoire physique protégée qui est utilisée par **iBoot** pour charger le noyau et les extensions de noyau. Après le démarrage, le contrôleur de mémoire interdit toute écriture dans la région de mémoire physique protégée. De plus, l'unité de gestion mémoire du processeur d'application (MMU) est configurée pour éviter le mappage de code privilégié de la mémoire physique à l'extérieur de la région de mémoire protégée et interdire tout mappage inscriptible de la mémoire physique au sein de la région de mémoire du noyau.

Le matériel utilisé pour le système KIP est verrouillé après le processus de démarrage afin d'éviter toute reconfiguration. Le système KIP est pris en charge à partir des SoC Apple A10 et S4.

Protection de l'intégrité des coprocesseurs système

Les coprocesseurs système sont des unités centrales de traitement placées sur le même SoC que le processeur d'application. Les coprocesseurs système sont consacrés à un objectif spécifique et le noyau iOS leur délègue de nombreuses tâches. Par exemple :

- Secure Enclave
- Processeur de capteur d'images
- Coprocesseur de mouvement

Comme le programme interne des coprocesseurs gère de nombreuses tâches système critiques, sa sécurité est un élément essentiel de la sécurité du système dans son ensemble.

La protection de l'intégrité des coprocesseurs système (SCIP) utilise un mécanisme semblable à la protection de l'intégrité du noyau pour éviter toute modification du programme interne des coprocesseurs. Au démarrage, iBoot charge le programme interne de chaque coprocesseur dans une région de mémoire protégée, réservée et séparée de la région KIP. iBoot configure les unités de gestion de mémoire de chaque coprocesseur pour éviter :

- les mappages exécutables en dehors de la partie de région de mémoire protégée qui lui est réservée ;
- les mappages inscriptibles dans sa partie de région de mémoire protégée.

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

Le matériel utilisé pour SCIP est verrouillé après le processus de démarrage afin d'éviter toute reconfiguration. SCIP est pris en charge à partir des SoC A12 et S4.

Codes d'authentification de pointeurs

Les codes d'authentification de pointeurs (Pointer authentication codes, ou PAC) sont utilisés pour assurer une protection contre toute exploitation des bugs d'altération de mémoire. Le logiciel système et les applications intégrées utilisent les PAC pour empêcher toute modification des pointeurs de fonction et des adresses de retour (pointeurs de code). Cela permet d'augmenter le niveau de difficulté de nombreuses attaques. Les attaques de type ROP (Return Oriented Programming), par exemple, tentent de tromper l'appareil pour l'amener à exécuter du code existant de manière malveillante en manipulant les adresses de retour de fonction stockées dans la pile.

Les PAC sont pris en charge sur les SoC 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 et à l'iPad. Cette technologie lit les données d'empreintes digitales sous n'importe quel angle et développe ses connaissances 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

Un seul coup d'œil suffit pour que Face ID déverrouille en toute sécurité un appareil Apple équipé de cette fonction. Elle fournit une authentification intuitive et sécurisée activée par le système photographique TrueDepth qui utilise des technologies avancées pour cartographier avec précision la géométrie de votre visage. Face ID utilise des réseaux de neurones pour la détermination de l'attention, la reconnaissance et la prévention de l'usurpation d'identité, afin que vous puissiez déverrouiller votre téléphone d'un simple coup d'œil. Face ID s'adapte automatiquement aux changements de votre apparence et protège la confidentialité et la sécurité de vos données biométriques.

Touch ID, Face ID et les codes de verrouillage

Pour utiliser Touch ID ou Face ID, vous devez configurer votre appareil de sorte qu'un code de verrouillage soit nécessaire pour le déverrouiller. Lorsque Touch ID ou Face ID repère une correspondance, votre appareil se déverrouille sans demander le code de verrouillage. Cela rend l'utilisation d'un code de verrouillage plus long et complexe beaucoup plus pratique, car vous n'avez pas besoin de le saisir aussi souvent. Touch ID et Face ID ne remplacent pas votre code de verrouillage. Ils facilitent simplement l'accès à votre appareil grâce à un compromis bien pensé entre sécurité et rapidité. Cela est important, car un code de verrouillage complexe constitue le fondement de la protection cryptographique de vos données par votre appareil iOS.

Vous pouvez utiliser Touch ID ou Face ID dans la plupart des cas, ou votre code de verrouillage si vous le préférez, mais les opérations suivantes exigent un code plutôt qu'une identification biométrique :

- Mise à jour de votre logiciel.
- Effacement du contenu de votre appareil.
- Affichage ou modification des réglages de code de verrouillage.
- Installation de profils de configuration iOS.

Un code de verrouillage est également exigé si votre appareil affiche l'un des 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 de verrouillage n'a pas été utilisé pour déverrouiller l'appareil au cours des 156 dernières heures (six jours et demi) et l'appareil n'a pas été déverrouillé par un moyen biométrique au cours des 4 dernières heures.
- L'appareil a reçu une commande de verrouillage à distance.
- Après cinq tentatives manquées de reconnaissance biométrique.
- Après une mise en arrêt/un appel d'urgence.

Lorsque Touch ID ou Face ID est activé, l'appareil se verrouille automatiquement lorsque vous appuyez sur le bouton latéral. Par ailleurs, l'appareil se verrouille chaque fois qu'il passe en mode veille. Touch ID et Face ID nécessitent une reconnaissance positive – ou l'introduction du code de verrouillage – à chaque réactivation de l'appareil.

La probabilité qu'un individu quelconque puisse déverrouiller votre iPhone est de 1 sur 50 000 avec Touch ID ou de 1 sur 1 000 000 avec Face ID. Cette probabilité augmente avec le nombre d'empreintes digitales enregistrées (jusqu'à 1 sur 10 000 avec cinq empreintes) ou d'apparences

enregistrées (jusqu'à 1 sur 500 000 avec deux apparences). Pour plus de protection, Touch ID et Face ID limitent le nombre d'échecs à cinq avant que l'appareil vous demande de saisir votre code de verrouillage pour vous permettre d'y accéder. Dans le cas de Face ID, la probabilité d'une fausse reconnaissance diffère pour les jumeaux et les frères et sœurs qui vous ressemblent et pour les enfants de moins de 13 ans, car il se peut que les traits de leur visage ne se soient pas encore complètement développés. Si cela vous préoccupe, Apple recommande l'usage d'un code de verrouillage pour s'authentifier.

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 à Secure Enclave. La communication entre le processeur et le capteur de Touch ID se produit à travers un bus d'interface périphérique série. Le processeur envoie les données au Secure Enclave sans pouvoir les lire. Les données sont chiffrées et authentifiées grâce à une clé de session qui est négociée en utilisant une clé partagée fournie à l'usine pour chaque capteur Touch ID et son Secure Enclave correspondant. La clé partagée est complexe, aléatoire et différente pour chaque capteur Touch ID. L'échange de la clé de session se fait à travers un **enveloppement (ou encapsulation) 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 supprimée. L'analyse fait appel à une **cartographie des angles des crêtes papillaires**, 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 Secure Enclave. Ces données ne quittent jamais l'appareil. Elles ne sont ni envoyées à Apple, ni incluses dans les sauvegardes de l'appareil.

Sécurité de Face ID

Face ID permet de confirmer l'attention de l'utilisateur, offre une authentification ultra-fiable avec un faible taux d'erreur de correspondance et réduit aussi bien l'usurpation d'identité numérique que physique.

L'appareil photo TrueDepth recherche automatiquement votre visage lorsque vous activez un appareil Apple équipé de la fonction Face ID en le levant ou en touchant l'écran, mais aussi lorsque cet appareil essaie de vous authentifier pour afficher une notification entrante ou lorsqu'une app prise en charge sollicite une identification par Face ID. Lorsqu'un visage est détecté, Face ID confirme l'attention et tente de déverrouiller l'appareil en s'assurant que vos yeux sont ouverts et que votre attention est dirigée vers lui. Pour des raisons d'accessibilité, cette fonction est désactivée lorsque VoiceOver est activé et peut, si nécessaire, être désactivée séparément.

Une fois la présence d'un visage attentif établie, l'appareil photo TrueDepth projette et lit plus de 30 000 points infrarouges pour cartographier les profondeurs du visage, ainsi qu'une image 2D infrarouge. Ces données sont utilisées pour créer une séquence d'images 2D et de cartes de profondeur qui sont numériquement signées puis envoyées au Secure Enclave. Pour contrer les usurpations d'identité numériques et physiques,

l'appareil photo TrueDepth ordonne de façon aléatoire la séquence d'images 2D et les captures de cartes de profondeur, puis projette un motif aléatoire propre à l'appareil. Une portion du moteur de neurones des SoC A11 et des modèles plus récents – protégée à l'intérieur du Secure Enclave – transforme ces données en une représentation mathématique et la compare aux données faciales enregistrées. Ces données faciales enregistrées sont une représentation mathématique de votre visage capturé dans différentes poses.

La reconnaissance faciale est réalisée dans le Secure Enclave à l'aide de réseaux de neurones spécialement formés pour cela. Nous avons développé les réseaux de neurones de reconnaissance faciale en utilisant plus d'un milliard d'images, dont des images infrarouges et de profondeur recueillies au cours d'études réalisées avec le consentement éclairé des participants. Apple a travaillé avec des volontaires du monde entier pour créer un groupe de personnes représentatif de tout sexe, âge, origine, etc. Les études ont été augmentées en fonction des besoins pour garantir une grande précision pour un éventail d'utilisateurs divers. La fonction Face ID a été conçue pour fonctionner avec des chapeaux, des écharpes, des lunettes, des lentilles de contact et de nombreuses lunettes de soleil. Par ailleurs, ce système de reconnaissance facial a été conçu pour fonctionner en intérieur, en plein air et même dans le noir le plus total. Un réseau de neurones supplémentaire, formé pour détecter et résister à l'usurpation d'identité, vous protège contre toute tentative de déverrouillage de votre iPhone X à l'aide de photos ou de masques.

Les données de Face ID, comprenant les représentations mathématiques de votre visage, sont chiffrées et seul le Secure Enclave y a accès. Ces données ne quittent jamais l'appareil. Elles ne sont ni envoyées à Apple, ni incluses dans les sauvegardes de l'appareil. Les données Face ID ci-dessous sont enregistrées et chiffrées pour n'être utilisées que par le Secure Enclave dans le cadre d'un fonctionnement normal :

- les représentations mathématiques de votre visage calculées pendant l'enregistrement ;
- les représentations mathématiques de votre visage calculées lors de certaines tentatives de déverrouillage si Face ID les juge utiles pour accroître les probabilités de reconnaissance à venir.

Les images faciales capturées pendant le fonctionnement normal de l'appareil ne sont pas enregistrées, mais sont supprimées après le calcul de la représentation mathématique en vue de son enregistrement ou pour la comparer avec les données enregistrées de Face ID.

Comment Touch ID ou Face ID déverrouille un appareil iOS

Lorsque Touch ID ou Face ID est désactivé, les clés de la plus haute classe de protection des données, conservées dans le Secure Enclave, sont supprimées lorsque l'appareil se verrouille. Les fichiers et les éléments du **trousseau** appartenant à cette classe restent inaccessibles jusqu'à ce que vous déverrouilliez l'appareil en saisissant votre code de verrouillage.

Lorsque Touch ID ou Face ID est activé, les clés ne sont pas supprimées lorsque l'appareil se verrouille ; elles sont cependant enveloppées à l'aide d'une clé attribuée au sous-système Touch ID ou Face ID, à l'intérieur de Secure Enclave. Si, lorsque vous essayez de le déverrouiller, l'appareil détecte une correspondance, il fournit la clé nécessaire pour déballer les clés de protection des données et se déverrouille. Ce processus fournit une protection supplémentaire en nécessitant la coopération entre les sous-systèmes de protection de données et Touch ID ou Face ID pour déverrouiller l'appareil.

Lorsque l'appareil redémarre, les clés requises pour que Touch ID et Face ID déverrouillent l'appareil sont perdues, le Secure Enclave les supprime après que les conditions nécessitant la saisie du code de verrouillage sont satisfaites (par exemple, après que l'appareil n'a pas été déverrouillé au cours des 48 dernières heures ou après cinq échecs de tentative de reconnaissance).

Pour améliorer la fonction de déverrouillage et l'aligner sur l'évolution naturelle des traits et apparence de votre visage, Face ID augmente, avec le temps, les représentations mathématiques stockées. Après un déverrouillage réussi, il se peut que Face ID utilise la représentation mathématique nouvellement calculée (si elle est d'une qualité suffisamment bonne) pour un nombre fini de déverrouillages supplémentaires avant que les données ne soient supprimées. Inversement, si Face ID ne vous reconnaît pas, mais que la qualité de la reconnaissance est supérieure à un seuil défini et que vous saisissez le code de verrouillage immédiatement après, Face ID effectue une nouvelle capture et affine la nouvelle représentation mathématique calculée à ses données enregistrées. Ces nouvelles données Face ID sont supprimées si vous cessez de les utiliser comme éléments de comparaison et après un nombre fini de déverrouillages. Ces processus d'augmentation permettent à Face ID de suivre les modifications substantielles de pilosité faciale ou de maquillage, tout en minimisant l'acceptation par erreur.

Touch ID, Face ID et Apple Pay

Vous pouvez utiliser Touch ID et Face ID avec Apple Pay pour effectuer facilement des achats sécurisés dans des boutiques, des apps et sur Internet. Pour en savoir plus sur Touch ID et Apple Pay, consultez la section Apple Pay de ce document.

Pour autoriser un paiement en magasin avec Face ID, vous devez tout d'abord confirmer l'intention de payer en double-cliquant sur le bouton latéral. Vous devez ensuite procéder à l'identification par Face ID avant de placer votre iPhone X près du lecteur de paiement sans contact. Si vous souhaitez sélectionner un autre moyen de paiement Apple Pay après authentification par Face ID, vous devez procéder à une nouvelle authentification, mais vous n'aurez alors pas besoin de double-cliquer à nouveau sur le bouton latéral.

Pour effectuer des paiements dans des apps et sur Internet, confirmez l'intention de payer en double-cliquant sur le bouton latéral, puis identifiez-vous à l'aide de Face ID pour autoriser le paiement. Si votre transaction Apple Pay n'est pas réalisée au plus tard 30 secondes après avoir appuyé deux fois sur le bouton latéral, vous devez confirmer une nouvelle fois l'intention de payer en double-cliquant à nouveau.

Face ID Diagnostics

Les données de Face ID ne quittent pas votre appareil et ne sont jamais sauvegardées sur iCloud ou ailleurs. Ce n'est que si vous souhaitez fournir des données de diagnostic de Face ID à AppleCare pour obtenir de l'assistance que ces informations sont transférées depuis votre téléphone. L'activation de Face ID Diagnostics requiert une autorisation numériquement signée d'Apple qui est similaire à celle utilisée dans le processus de personnalisation des mises à jour de logiciels. Après l'autorisation, vous pouvez activer Face ID Diagnostics et entamer la procédure de configuration depuis l'app Réglages sur les appareils qui prennent en charge Face ID.

Pendant la configuration de Face ID Diagnostics, votre enregistrement existant est supprimé et vous êtes invité à vous réenregistrer. Les appareils qui prennent en charge Face ID commencent à enregistrer les images capturées pendant les tentatives d'authentification par Face ID au cours des 10 jours suivants, après quoi, ils cessent automatiquement d'enregistrer toute image. Face ID Diagnostics n'envoie pas automatiquement des données à Apple. Vous pouvez revoir et approuver l'enregistrement et déverrouiller les images (réussies ou manquées) incluses dans les données de diagnostic Face ID collectées en mode diagnostic avant qu'elles ne soient envoyées à Apple. Face ID Diagnostics ne télécharge vers Apple que les images Face ID Diagnostics que vous avez approuvées. Les données sont chiffrées avant leur téléchargement et immédiatement supprimées de l'appareil une fois le téléchargement effectué. Les images rejetées sont immédiatement supprimées.

Si vous ne terminez pas la session Face ID Diagnostics en passant les images en revue et en téléchargeant les images approuvées, Face ID Diagnostics cesse automatiquement après 40 jours et toutes les images de diagnostic sont éliminées de l'appareil. Vous pouvez également désactiver Face ID Diagnostics à tout moment. Toutes les images locales sont immédiatement supprimées si vous optez pour cette solution et, dans un tel cas de figure, aucune donnée de Face ID n'est partagée avec Apple.

Autres usages de Touch ID et Face ID

Les applications tierces peuvent utiliser des API système pour demander à l'utilisateur de s'identifier par Touch ID, Face ID ou un code de verrouillage. Les applications prenant en charge Touch ID sont également compatibles avec Face ID sans aucune 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 accéder ni à Touch ID, ni à Face ID, ni aux données associées à l'utilisateur enregistré. Les éléments du trousseau peuvent également être protégés avec Touch ID ou Face ID. Dans un tel contexte, Secure Enclave ne permet d'y accéder qu'en cas de correspondance ou si le code de verrouillage de l'appareil est saisi. Les développeurs d'app disposent d'API pour vérifier qu'un code de verrouillage a été défini par l'utilisateur, avant de solliciter Touch ID, Face ID ou un code de verrouillage pour déverrouiller des éléments du trousseau. Les développeurs peuvent effectuer les opérations suivantes :

- L'échec des opérations d'authentification au travers des API n'oblige pas à saisir le mot de passe d'une application ou le code de verrouillage d'un appareil. Ils peuvent déterminer si un utilisateur est enregistré, ce qui permet à Touch ID ou à Face ID d'être utilisé comme second facteur dans les applications ultrasensibles.
- Ils sont en mesure de générer et d'utiliser, au sein du Secure Enclave, des clés ECC qui peuvent être protégées par Touch ID ou Face ID. Les opérations avec ces clés sont systématiquement réalisées à l'intérieur du Secure Enclave après que ce dernier autorise leur utilisation.

Vous pouvez aussi configurer Touch ID ou Face ID pour autoriser des achats dans l'iTunes Store, l'App Store et Apple Books, et ainsi éviter aux utilisateurs d'avoir à saisir un mot de passe d'identifiant Apple. Sous iOS 11 ou ultérieur, les clés ECC du Secure Enclave protégées par Touch ID et Face ID permettent d'autoriser un achat en signant la requête du Store.

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 l'espace d'Effaceable Storage, rendant ainsi cryptographiquement inaccessibles 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 le transmettre 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 (sur un appareil comportant des modifications non autorisées, par exemple). 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 du matériel

Sur les appareils mobiles, la vitesse et l'efficacité énergétique sont essentielles. Les opérations cryptographiques sont complexes et peuvent engendrer des problèmes de performances ou d'autonomie de la batterie si elles ne sont pas conçues et implémentées 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 ultérieurs de la série A, le sous-système de stockage Flash se trouve sur un bus isolé qui ne peut accéder à la mémoire contenant les données utilisateur qu'à travers le moteur de chiffrement DMA.

Les **identifiants uniques (UID)** et les **identifiants de groupe (GID)** d'un appareil sont des clés AES-256 bits fusionnées (UID) ou compilées (GID) dans le processeur d'application et 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 possèdent chacun leur propre UID et leur propre GID. En outre, l'UID et le GID du Secure Enclave ne peuvent être utilisés que par le moteur AES dédié au Secure Enclave. Les UID et les GID ne sont pas non plus accessibles via **JTAG (Joint Test Action Group)** ou d'autres interfaces de débogage.

À l'exception des SoC Apple A8 et antérieures, chaque Secure Enclave génère son propre UID (identifiant unique) durant le processus de fabrication. Dans la mesure où chaque appareil dispose de son propre UID et comme ce dernier est entièrement généré au sein du Secure Enclave plutôt que dans un système de fabrication extérieur à l'appareil, l'UID n'est ni accessible ni stockable par Apple ou l'un de ses fournisseurs.

Le logiciel exécuté sur le Secure Enclave utilise l'UID pour protéger les secrets de l'appareil. L'UID permet de lier cryptographiquement des données à un appareil précis. Par exemple, la hiérarchie des clés protégeant le système de fichiers inclut l'UID ; donc, 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.

Le GID est commun à tous les processeurs d'une classe d'appareils (par exemple, tous les appareils utilisant le processeur Apple A8).

Hormis l'UID et le GID, toutes les autres clés cryptographiques sont créées par le générateur de nombres aléatoires (RNG, Random Number Generator) du système à l'aide d'un algorithme basé sur le code source CTR_DRBG. L'entropie du système est générée à partir des variations temporelles lors du démarrage, et à partir du temps entre les interruptions une fois l'appareil démarré. Les clés générées à l'intérieur de la puce Secure Enclave utilisent son générateur de nombres aléatoires matériel s'appuyant sur plusieurs oscillateurs en anneau post-traités par CTR_DRBG.

L'effacement sécurisé des clés enregistrées est tout aussi important que leur génération. Cela s'avère particulièrement délicat dans le stockage Flash, où le contrôle d'usure peut nécessiter, par exemple, 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 **Effaceable Storage**. 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 ne fonctionne pas car l'iPhone doit être rechargé, il se peut que la batterie dispose de suffisamment d'énergie pour prendre en charge des transactions de carte Express.

Les appareils iPhone compatibles prennent automatiquement cette fonction en charge avec :

- les cartes de transport désignées comme cartes de transport Express ;
- les cartes d'étudiant dont le mode Express est activé.

Appuyer sur le bouton latéral permet d'afficher l'icône de batterie faible et un texte indiquant les cartes Express qui peuvent être utilisées. Le contrôleur NFC effectue les transactions de carte Express dans les mêmes conditions que si iOS était en cours d'exécution, à la différence près que les transactions sont notifiées uniquement par des vibrations. Aucune notification visuelle n'est affichée.

Cette fonction n'est pas disponible lorsque l'appareil est éteint de manière normale par l'utilisateur.

Protection des données des fichiers

En plus des fonctionnalités de chiffrement matériel intégrées aux appareils iOS, Apple utilise une technologie appelée Data Protection 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 ultérieur bénéficient automatiquement de cette protection.

La protection des données est implémentée en construisant et en gérant une hiérarchie de clés, et repose sur les technologies de chiffrement matériel intégrées à chaque appareil iOS. La protection des données 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'apparition d'Apple File System (APFS), le système de fichiers est dorénavant capable de subdiviser davantage les données en plusieurs morceaux (des portions de fichier peuvent avoir plusieurs clés).

Vue d'ensemble de l'architecture

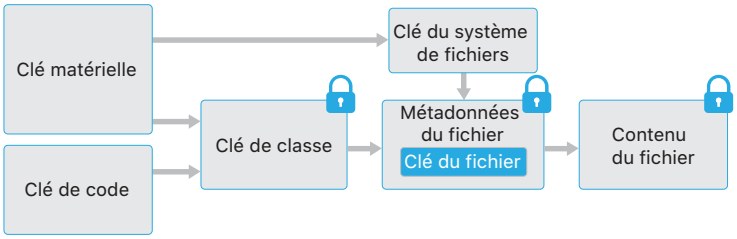
Chaque fois qu'un fichier est créé sur la partition de données, la protection des données crée une nouvelle clé 256 bits (la clé « par fichier ») et la transmet au moteur AES matériel qui l'utilise alors pour chiffrer le fichier lors de son écriture dans la mémoire Flash en utilisant le mode AES-XTS.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

La clé par fichier (ou par morceau) est enveloppée à l'aide d'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 fonctionnant au format Apple File System peuvent prendre en charge le clonage des fichiers (des copies à coût zéro utilisant la technologie de copie sur écriture). Si un fichier est cloné, chaque moitié du clone obtient une nouvelle clé pour accepter les écritures entrantes de manière que les nouvelles données soient inscrites sur le support avec une nouvelle clé. Avec le temps, le fichier peut être composé de plusieurs morceaux (ou fragments) correspondant chacune à des clés différentes. Cependant, tous les morceaux qui comprennent un fichier sont conservés par la même clé de la classe.

Lorsqu'un fichier est ouvert, ses métadonnées sont déchiffrées avec la **clé du système de fichiers**, révélant la clé enveloppée par fichier et une notation sur laquelle la classe la protège. La clé par fichier (ou par morceau) est désenveloppée à l'aide de la clé de classe, puis transmise au moteur AES matériel, qui déchiffre le fichier lors de sa lecture depuis la mémoire Flash. Toute la gestion des clés de fichier enveloppées se produit dans Secure Enclave ; la clé de fichier n'est jamais directement exposée au processeur d'application. Au démarrage, Secure Enclave négocie une clé éphémère avec le moteur AES. Lorsque Secure Enclave désenveloppe les clés d'un fichier, elle utilise pour cela la clé éphémère puis renvoie les clés 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. Dans le cas des appareils qui prennent en charge le système AFS (Apple File System), la clé des métadonnées du système de fichiers est enveloppée par la clé UID du Secure Enclave pour un stockage à long terme. Tout comme pour les clés par fichier ou par morceau, la clé des métadonnées n'est jamais directement exposée au processeur d'application ; le Secure Enclave fournit plutôt une version éphémère par démarrage. Lorsqu'il est stocké, le système de fichiers chiffré est par ailleurs enveloppé par une « clé effaçable ». Cette clé ne permet pas de renforcer la confidentialité des données. Elle est en fait conçue pour être rapidement effacée à la 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 travers une solution MDM, 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 une ou plusieurs clés de fichier (ou de morceau) qui sont enveloppées avec une clé de classe et stockées dans les métadonnées d'un fichier qui sont, à leur tour, chiffrées à l'aide de la clé du système de fichiers. La clé de classe est protégée par l'UID du matériel et, pour certaines classes, le code de verrouillage 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 réenveloppant sa clé par fichier, et la modification du code de verrouillage ne réenveloppe que la clé de classe.

Codes de verrouillage

En configurant un code de verrouillage d'appareil, l'utilisateur active automatiquement la protection des données. iOS prend en charge les codes à six chiffres, à quatre chiffres et alphanumériques de longueur arbitraire. En plus de déverrouiller l'appareil, un code de verrouillage 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 spécifiques sans le code de verrouillage.

Le code de verrouillage étant combiné à l'UID de l'appareil, des attaques par force brute 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. Cela signifie qu'il faudrait plus de cinq ans et demi pour essayer toutes les combinaisons de code à six caractères alphanumériques.

Plus le code de verrouillage 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 définir un code de verrouillage beaucoup plus complexe qu'il ne le ferait en temps

Remarques à propos du code de verrouillage

En cas de saisie d'un code de longueur importante ne contenant que des chiffres, un pavé numérique est affiché sur l'écran de verrouillage au lieu du clavier complet. Un code de verrouillage 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 de verrouillage

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

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 plus les attaques par force brute, des délais de plus en plus longs sont prévus après la saisie d'un code de verrouillage 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 10 tentatives infructueuses consécutives de saisie du code de verrouillage. Les tentatives consécutives de saisie du même code de verrouillage incorrect ne sont pas comptabilisées pour la limite autorisée. Ce réglage est également disponible sous forme de règle administrative via une solution MDM qui prend en charge cette fonction et Exchange ActiveSync, tandis que son seuil peut être abaissé.

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

Pour renforcer la sécurité tout en maintenant la facilité d'utilisation, iOS 11.4.1 ou ultérieur nécessite Touch ID, Face ID ou la saisie d'un code de verrouillage pour activer l'interface USB si l'USB n'a pas été utilisé récemment. Cela permet d'éliminer la surface d'attaque contre des appareils physiquement connectés tels que des chargeurs malveillants tout en permettant toujours l'utilisation d'accessoires USB dans des délais raisonnables. S'il s'est écoulé plus d'une heure depuis le verrouillage de l'appareil iOS ou depuis la déconnexion d'un périphérique USB, l'appareil n'autorise aucune nouvelle connexion tant que l'appareil n'a pas été déverrouillé. Cette période d'une heure :

- permet de s'assurer que les utilisateurs fréquents de connexions filaires CarPlay ou de connexions à un Mac, un PC ou des accessoires USB ne sont pas obligés de saisir leur code de verrouillage chaque fois qu'ils connectent leur appareil ;
- est nécessaire car l'écosystème d'accessoires USB ne fournit pas de moyen fiable pour identifier les accessoires avant d'établir une connexion de données.

De plus, sous iOS 12, si plus de trois jours se sont écoulés depuis l'établissement d'une connexion USB, l'appareil refuse toute nouvelle connexion USB immédiatement après son verrouillage. Cela a pour but de renforcer la protection des utilisateurs qui n'utilisent pas souvent ce type de connexion. Les connexions USB sont également désactivées chaque fois que l'appareil se trouve dans un état qui nécessite le code de verrouillage pour réactiver l'authentification biométrique.

L'utilisateur peut choisir de réactiver les connexions USB permanentes dans Réglages ; la configuration de certains dispositifs d'aide effectue ce réglage automatiquement.

Mode de récupération et mode DFU

Sur les appareils équipés de SoC Apple A10, A11 et S3, il est impossible d'utiliser le mode de récupération pour accéder aux clés de classe protégées par le code de verrouillage de l'utilisateur. Les SoC A12 et S4 étendent cette protection au mode DFU.

Le moteur AES du Secure Enclave est équipé de bits d'amorçage logiciel verrouillables. Lorsque des clés sont créées à partir de l'UID, ces bits d'amorçage sont inclus dans la fonction de dérivation de clés afin de créer des hiérarchies de clés supplémentaires.

À partir des SoC Apple A10 et S3, un bit d'amorçage est spécialement utilisé pour distinguer les clés protégées par le code de verrouillage de l'utilisateur. Le bit d'amorçage est activé pour les clés qui exigent le code de verrouillage de l'utilisateur (ce qui comprend les clés de protection de données de classe A, de classe B et de classe C) et désactivé pour les clés qui n'exigent pas le code de verrouillage d'utilisateur (ce qui comprend la clé de métadonnées du système de fichiers et les clés de classe D).

Sur les SoC A12, la ROM de démarrage Secure Enclave verrouille le bit d'amorçage du code de verrouillage si le processeur d'application est passé en mode DFU ou en mode de récupération. Lorsque le bit d'amorçage du code de verrouillage est verrouillé, aucune opération de modification n'est autorisée, ce qui interdit l'accès aux données protégées à l'aide du code de verrouillage de l'utilisateur.

Sur les SoC Apple A10, A11, S3 et S4, le bit d'amorçage du code est verrouillé par le système d'exploitation Secure Enclave si l'appareil est passé en mode de récupération. La ROM de démarrage et le système d'exploitation Secure Enclave vérifient tous les deux le registre de progression du démarrage pour déterminer en toute sécurité le mode en cours.

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.

Complete Protection

(`NSFileProtectionComplete`) : la clé de classe est protégée par une clé obtenue à partir du code de verrouillage de l'utilisateur et de l'UID de l'appareil. Peu après que l'utilisateur verrouille un appareil (10 secondes, si le paramètre Exiger le mot de passe est défini sur Immédiatement), la clé de la classe déchiffrée est éliminée, rendant toutes les données de cette classe inaccessible jusqu'à ce que l'utilisateur saisisse à nouveau le code ou déverrouille l'appareil par Touch ID ou Face ID.

Protected Unless Open

(`NSFileProtectionCompleteUnlessOpen`) : certains fichiers peuvent nécessiter d'être écrits pendant que l'appareil est verrouillé. Cela est le cas, par exemple, lors du téléchargement d'une pièce jointe en arrière-plan. Ce comportement peut être obtenu grâce à la cryptographie asymétrique à courbes elliptiques (ECDH sur Curve25519). La clé de fichier habituelle est protégée par une clé obtenue au moyen de l'échange de clés 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 une fonction de dérivation de clé de concaténation (alternative approuvée 1) comme décrit 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 et de la clé publique éphémère du fichier, lesquelles servent à désenvelopper la clé par fichier permettant ainsi de déchiffrer le fichier.

Protected Until First User Authentication

(`NSFileProtectionCompleteUntilFirstUserAuthentication`) : cette classe se comporte comme la classe Complete Protection, sauf que la clé de classe déchiffrée n'est pas supprimée de la mémoire lorsque l'appareil est verrouillé. Cette classe présente des propriétés de protection similaires à celles du chiffrement de volume complet de l'environnement de bureau et protège les données des attaques impliquant un redémarrage. Il s'agit de la classe par défaut pour toutes les données d'apps tierces auxquelles aucune classe de protection des données n'est spécifiquement affectée.

No Protection

(`NSFileProtectionNone`) : cette clé de classe n'est protégée que par l'UID et est conservée dans l'Effaceable Storage. Comme toutes les clés nécessaires au déchiffrement des fichiers appartenant à cette classe sont stockées sur l'appareil, le chiffrement n'apporte comme avantage que la possibilité d'effacement à distance rapide. Si aucune classe de protection des données n'est affectée à un fichier, celui-ci est tout de même stocké sous forme chiffrée (comme toutes les données d'un appareil iOS).

Clé de la classe de protection des données

Classe A	Complete Protection	(NSFileProtectionComplete)
Classe B	Protected Unless Open	(NSFileProtectionCompleteUnlessOpen)
Classe C	Protected Until First User Authentication	(NSFileProtectionCompleteUntilFirstUserAuthentication)
Classe D	No Protection	(NSFileProtectionNone)

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 à l'aide de deux clés AES-256-GCM différentes, 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 une clé de métadonnées pour accélérer la recherche, tandis que la valeur secrète (kSecValueData) est chiffrée à l'aide d'une clé secrète séparée. La clé de métadonnées est protégée par le processeur Secure Enclave, mais mise en cache dans le processeur d'application pour autoriser des recherches rapides sur le contenu du trousseau. La clé secrète requiert toujours un aller-retour à travers le processeur Secure Enclave.

Le trousseau est implémenté sous la forme d'une base de données SQLite stockée sur le système de fichiers. Il n'existe qu'une seule base de données et le daemon *securityd* détermine les éléments du trousseau auxquels chaque processus ou app peut accéder. Les API d'accès au

Composants d'un élément de trousseau

Chaque élément de trousseau contient, en plus du groupe d'accès, des métadonnées administratives (comme des horodatages de création et de dernière modification).

Il contient également les hachages SHA-1 des attributs utilisés pour demander l'élément (tels que le nom du compte et le nom du serveur), afin de permettre la recherche sans devoir déchiffrer chaque élément. Enfin, il contient les données de chiffrement qui incluent les éléments suivants :

- 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 avec la clé de classe de protection ;
- dictionnaire d'attributs décrivant l'élément (tel que transmis à SecItemAdd), codé 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 Mode) ; le groupe d'accès est inclus dans les attributs et protégé par la balise GMAC calculée pendant le chiffrement.

trousseau envoient des appels au daemon, lequel interroge les droits « groupes d'accès au trousseau », « identifiant d'application » et « groupe d'application » 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 implémentée en obligeant les apps tierces à utiliser des groupes d'accès portant un préfixe qui leur est alloué par le biais du programme Apple Developer Program à travers les groupes d'applications. L'obligation d'utiliser un préfixe et le caractère unique du groupe d'applications sont contrôlés par la signature du code, des **profils d'approvisionnement** et le programme Apple Developer Program.

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 Authentification Initiale	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Toujours	NSFileProtectionNone	kSecAttrAccessibleAlways
Code de verrouillage 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 de verrouillage est configuré pour l'appareil. Cette classe n'existe que dans le **conteneur de clés** du système ; elle :

- n'est pas synchronisée avec le trousseau iCloud ;
- n'est pas sauvegardée ;
- n'est pas incluse dans le conteneur de clés de dépôt.

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

D'autres classes du trousseau ont un équivalent « Cet appareil uniquement » qui est toujours protégé par l'UID quand il est copié depuis 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 déterminant le moment où iOS en a besoin. 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 Authentification Initiale
Comptes Mail	Après Authentification Initiale
Comptes Exchange	Après Authentification Initiale
Mots de passe VPN	Après Authentification Initiale
LDAP, CalDAV, CardDAV	Après Authentification Initiale
Jetons des comptes de réseau social	Après Authentification Initiale
Clés de chiffrement des annonces Handoff	Après Authentification Initiale
Jeton iCloud	Après Authentification Initiale
Mot de passe de partage à domicile	Lorsque l'appareil est déverrouillé
Jeton Localiser mon iPhone	Toujours
Messagerie	Toujours
Sauvegarde iTunes	Lorsque l'appareil est déverrouillé, non itinérant
Mots de passe Safari	Lorsque l'appareil est déverrouillé
Signets Safari	Lorsque l'appareil est déverrouillé
Certificats VPN	Toujours, non itinérant
Clés Bluetooth®	Toujours, non itinérant
Jeton du service Apple Push Notification	Toujours, non itinérant
Certificats et clé privée iCloud	Toujours, non itinérant
Clés iMessage	Toujours, non itinérant
Certificats et clés privées installés par le profil de configuration	Toujours, non itinérant
Code PIN de la carte SIM	Toujours, non itinérant

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, Face ID ou en saisissant le code de verrouillage de l'appareil. L'accès aux éléments peut également être limité 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 ACL sont évaluées à l'intérieur de Secure Enclave et ne sont transmises au noyau que si leurs 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 de verrouillage est saisi, la clé `NSFileProtectionComplete` est chargée depuis le conteneur de clés du système et désenveloppée. Il s'agit d'un fichier de liste de propriétés (.plist) binaire appartenant à la classe No Protection, dont le contenu est chiffré à l'aide d'une clé conservée dans l'Effaceable Storage. 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 de verrouillage. 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 désenveloppées.

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 verrouillage de l'utilisateur devient obligatoire. iOS ne prend pas en charge la séparation cryptographique du contenu du système de fichiers pour chaque 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 verrouillage 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 à nouveau chiffrées avec ces nouvelles clés. Comme expliqué précédemment, les éléments du trousseau non itinérants restent enveloppés avec la clé dérivée 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 10 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 par force brute 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 la gestion d'appareils mobiles (MDM). Ce conteneur de clés permet à iTunes de réaliser des sauvegardes et des synchronisations sans nécessiter la saisie d'un code de verrouillage par l'utilisateur, et à une solution MDM d'effacer à distance le code d'un utilisateur. Il est stocké sur l'ordinateur utilisé pour effectuer la synchronisation avec iTunes, ou sur la solution MDM 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 de verrouillage, 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 Protected Until First User Authentication. C'est pourquoi le code de verrouillage 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 en mode OTA (Over-The-Air), l'utilisateur est invité à saisir son code de verrouillage 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 verrouillage 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 Secure Enclave, de l'UUID du conteneur de clés et de l'UID de 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 l'authentification initiale d'un appareil redémarré, lorsqu'une mise à jour logicielle est annulée (par l'utilisateur ou par le système) ou quand le délai de la politique de temps d'un jeton a expiré.

Le jeton de déverrouillage à usage unique pour les mises à jour surveillées de logiciel expire au bout de 20 minutes. Ce jeton est exporté depuis le Secure Enclave, puis inscrit sur l'Effaceable Storage. Le délai d'une politique de temps incrémente le compteur si l'appareil n'a pas redémarré dans les 20 minutes.

Les mises à jour logicielles sans surveillance sont effectuées dès que le système détecte la disponibilité d'une mise à jour et :

- les mises à jour automatiques sont configurées sous iOS 12 ;

  ou

- l'utilisateur choisit « Installer plus tard » lorsqu'il est averti de la mise à jour.

Après la saisie du code de verrouillage par l'utilisateur, un jeton de déverrouillage ponctuel est généré et peut demeurer valide dans le Secure Enclave pendant 8 heures au maximum. Si la mise à jour n'a pas encore eu lieu, ce jeton de déverrouillage ponctuel est supprimé à chaque verrouillage et recréé à chaque déverrouillage suivant. Chaque déverrouillage relance la fenêtre de 8 heures.

Après 8 heures, une politique de temps invalide le jeton de déverrouillage ponctuel.

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 Protected Unless Open Data Protection), les sauvegardes iCloud peuvent être réalisées en arrière-plan. Pour toutes les classes de protection des données, à l'exception de No 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 termes de productivité, elles sont aussi susceptibles d'avoir un impact 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 en environnement « sandbox » 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. Les utilisateurs peuvent ainsi 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 tierces de charger du code non signé ou d'utiliser du code automodifiant.

Pour pouvoir développer et installer des apps sur des appareils iOS, les développeurs doivent s'enregistrer auprès d'Apple et adhérer au programme Apple Developer Program. 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 une personne ou une entreprise identifiable, ce qui dissuade de créer des apps malveillantes. Elles sont également vérifiées par Apple afin de s'assurer qu'elles fonctionnent comme décrit et ne présentent pas de bugs évidents ou d'autres problèmes. En plus des technologies déjà abordées, ce processus de curation garantit aux clients la qualité des apps qu'ils achètent.

iOS permet aux développeurs d'incorporer des frameworks dans leurs apps ; ceux-ci peuvent être utilisés par l'app elle-même ou par des extensions intégrées à celle-ci. Pour empêcher le système et les autres apps de charger du code tiers dans leur espace d'adressage, le système procède à la validation de la signature du code de toutes les bibliothèques dynamiques auxquelles un processus se lie lors de son lancement. Cette validation est réalisée par le biais de l'identifiant d'équipe (Team ID) issu d'un certificat émis par Apple. Un identifiant d'équipe est une chaîne

alphanumérique comportant 10 caractères ; par exemple, 1A2B3C4D5F. Un programme peut se lier 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 se lier 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 Developer Enterprise Program (ADEP) avec un numéro D-U-N-S. Apple accepte les candidats après validation de leur identité et de leur admissibilité. Une fois qu'un organisme est membre de l'ADEP, il peut s'enregistrer 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 par MDM sont considérées implicitement comme fiables, car la relation entre l'organisme 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, l'appareil doit recevoir la confirmation d'Apple que l'app est autorisée à s'exécuter.

Contrairement aux autres plates-formes mobiles, iOS n'autorise les utilisateurs ni à installer des apps non signées potentiellement malveillantes depuis des sites web, ni à exécuter du code non approuvé. Lors de l'exécution, des contrôles de signature du code de toutes les pages mémoire 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 tierces sont placées en environnement « sandbox » afin qu'elles ne puissent ni accéder aux fichiers stockés par les autres apps, ni apporter de modifications à l'appareil. Cela 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 tierce 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 tierces. L'ensemble de la partition du système d'exploitation est monté en lecture seule. Les outils qui ne sont pas indispensables, comme les services 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 le système iOS.

L'accès aux informations de l'utilisateur et à des fonctionnalités comme iCloud, ainsi que l'extensibilité par les apps tierces est contrôlé à l'aide de droits déclarés (entitlements). Les droits sont des paires clé-valeur signées intégrées à une app et permettent l'authentification au-delà des facteurs d'exécution, comme l'identifiant utilisateur Unix. Comme les droits sont signés numériquement, ils ne peuvent pas être modifiés. Les droits sont très utilisés par les apps et les daemons 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 daemon système compromis.

En outre, les apps ne peuvent réaliser un traitement en arrière-plan que par le biais des API fournies par le système. Cela leur permet de continuer à fonctionner sans affecter les performances ni réduire de façon importante l'autonomie de la batterie.

La randomisation du format d'espace d'adresse (ASLR, Address Space Layout Randomization) empêche l'exploitation des bugs de corruption de mémoire. Les apps intégrées utilisent l'ASLR pour garantir la randomisation 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 nombreuses exploitations sophistiquées. Par exemple, une attaque de type return-to-libc tente d'amener un appareil à exécuter un code malveillant en manipulant les adresses mémoire de la pile et des bibliothèques système. La randomisation de l'organisation 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 randomisée. 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*. Les extensions sont des exécutables binaires signés ayant une fonction spéciale incorporés dans une app. 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 droits peuvent être utilisés 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 framework système. Elles n'ont accès ni aux fichiers, ni aux espaces mémoire de l'autre. Les extensions sont conçues pour être isolées l'une de l'autre, de l'app contenante et des apps qui les utilisent. Elles sont placées en environnement « sandbox » comme toute autre app tierce et possèdent un conteneur distinct de celui de l'app contenante. Toutefois, elles partagent le même accès aux contrôles de confidentialité que cette dernière. Ainsi, si un utilisateur autorise une app à accéder aux Contacts, cette autorisation est étendue aux extensions intégrées à l'app, mais pas aux extensions activées par l'app.

Les claviers personnalisés sont un type d'extension spécifique étant donné que ces extensions sont activées par l'utilisateur pour l'ensemble du système. Une fois activée, une extension de clavier est utilisée pour toute saisie de texte, à l'exception du code de déverrouillage et de tout autre texte saisi dans un champ sécurisé. Pour limiter le transfert de données de l'utilisateur, les claviers personnalisés s'exécutent par défaut dans un environnement « sandbox » 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 Open Access, ce qui permet au système de l'exécuter dans l'environnement « sandbox » par défaut après obtention du consentement de l'utilisateur.

Pour les appareils enregistrés auprès d'une solution MDM, les extensions de document et de clavier obéissent aux règles de gestion d'ouverture de fichier (Managed Open In). Par exemple, la solution MDM 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 à un même groupe d'apps. Il appartient au développeur de créer les groupes appropriés sur le portail Apple Developer et d'inclure les apps et les extensions souhaitées. Une fois intégrées à un groupe d'apps, les apps ont accès à ce qui suit :

- 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 groupes 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 des apps et les données de localisation sont également stockées sous forme chiffrée avec des clés protégées par le code de verrouillage de l'utilisateur sur son appareil. Les apps Calendrier (à l'exception des pièces jointes), Contacts, Rappels, Notes, Messages et Photos implémentent le droit de protection des données Protected Until First User Authentication.

Les apps installées par l'utilisateur qui n'optent pas pour une classe de protection des données spécifique reçoivent par défaut la classe Protected Until First User Authentication.

Accessoires

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

Lorsqu'un accessoire MFi communique avec un appareil iOS par le biais 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 challenge 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 appareils 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 publique-privée 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. HomePod et Apple TV reçoivent des clés par le biais du mode « toucher pour configurer » ou du mode de configuration décrit ci-dessous. Les clés sont partagées depuis un iPhone avec une Apple Watch associée via le 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 (3072 bits), en utilisant un code à huit chiffres fourni par le fabricant de l'accessoire, saisi sur l'appareil iOS par l'utilisateur, puis chiffrées 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 qui ne possèdent pas de puce MFi peuvent intégrer la prise en charge de l'authentification logicielle sous iOS 11.3 ou une version ultérieure.

Lorsque l'appareil iOS et l'accessoire HomeKit communiquent, chacun authentifie l'autre en utilisant les clés échangées comme décrit 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 chiffrement de diffusion fournie par un appareil iOS associé via une session sécurisée. Cette clé est utilisée pour chiffrer les données relatives aux changements d'état de l'accessoire qui sont notifiées au moyen d'annonces Bluetooth Low Energy. La clé de chiffrement de diffusion est une clé dérivée HKDF-SHA-512 et les données sont chiffrées à l'aide d'un algorithme Authenticated Encryption with Associated Data (AEAD) ChaCha20-Poly1305. La clé de chiffrement de diffusion est remplacée régulièrement par l'appareil iOS et synchronisée avec d'autres appareils via iCloud conformément à la description présentée à 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 Protected Until First User Authentication. Les données HomeKit ne sont sauvegardées que sous forme chiffrée ; 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 iCloud.

Les données HomeKit sont également synchronisées entre plusieurs utilisateurs du même domicile. Ce processus fait appel à une authentification et 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, toute communication ultérieure est authentifiée et chiffrée à l'aide du protocole Station-to-Station et des clés par session.

L'utilisateur ayant initialement créé le domicile dans HomeKit ou tout autre utilisateur bénéficiant d'autorisations de modification peut 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 bénéficiant d'autorisations de modification ajoute un nouvel utilisateur, le processus est délégué à un concentrateur domestique pour terminer l'opération.

La procédure d'activation de l'Apple TV en vue d'une utilisation avec HomeKit est réalisée automatiquement si l'utilisateur se connecte à iCloud. Le compte iCloud nécessite l'activation de l'identification à deux facteurs. Apple TV et l'appareil de l'utilisateur (du propriétaire) échange des clés publiques temporaires Ed25519 sur iCloud. Lorsque l'appareil du propriétaire et l'Apple TV se trouvent sur le même réseau local, les clés temporaires servent à sécuriser une connexion à travers le réseau local en utilisant le protocole Station-to-Station et des clés de session. Ce processus fait appel à une authentification et un chiffrement identiques à ceux utilisés entre un appareil iOS et un accessoire HomeKit. Par le biais de cette connexion locale sécurisée, l'appareil du propriétaire transfère à l'Apple TV la paire de clés Ed25519 publique-privée de l'utilisateur. Ces clés sont ensuite utilisées pour sécuriser les transmissions entre l'Apple TV et les accessoires HomeKit, mais aussi entre l'Apple TV et les autres appareils iOS intégrant le domicile HomeKit.

Si un utilisateur n'a qu'un seul appareil et qu'il refuse 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 le nom des pièces et des accessoires, savoir dans quelle pièce se trouve chaque accessoire et accéder à d'autres informations, comme décrit en détail dans la documentation du développeur HomeKit à l'adresse : 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 concernant la configuration du domicile est fourni de façon anonyme à Siri afin de communiquer le nom des pièces, des accessoires et des scènes nécessaires à la reconnaissance des commandes. Il se peut que le son envoyé à Siri fasse état d'accessoires ou de commandes spécifiques, mais ces données Siri ne sont pas associées aux autres fonctionnalités Apple comme HomeKit. Pour en savoir plus, reportez-vous à « Siri » dans la section « Services Internet » de ce document.

Caméras IP de HomeKit

Les caméras IP de HomeKit envoient directement des flux vidéo et audio à l'appareil iOS sur le réseau local ayant accès au flux. Les flux sont chiffrés en utilisant des clés générées de manière aléatoire sur l'appareil iOS et la caméra IP, qui sont échangées lors de la session HomeKit sécurisée avec la caméra. Lorsque l'appareil iOS n'est pas sur le réseau local, les flux chiffrés sont relayés via le concentrateur domestique vers l'appareil iOS. Le concentrateur domestique ne déchiffre pas les flux et fonctionne uniquement comme relais entre l'appareil iOS et la caméra IP. Lorsqu'une app affiche la vidéo de la caméra IP HomeKit sur l'écran de l'utilisateur, HomeKit effectue le rendu des trames vidéo en toute sécurité à partir d'un processus système distinct de manière que l'app soit incapable d'y accéder ou de les stocker. Par ailleurs, les apps ne sont pas autorisées à effectuer des captures d'écran à partir 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 activés 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 challenge 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 challenge signé et du certificat X.509 du coprocesseur d'authentification. Ceux-ci servent à demander un certificat pour l'accessoire depuis le 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 autres informations nécessaires pour la connexion au serveur d'accès distant à iCloud. Ces informations ne sont pas spécifiques à un utilisateur ou 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 attribue aux utilisateurs un identifiant 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 des identifiants émis par iCloud, mais ces identifiants sont opaques et ne révèlent 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 ticket. Ce ticket est obtenu auprès d'un serveur iCloud différent ; celui-ci n'est pas unique à chaque accessoire. Lorsqu'un accessoire demande un ticket, 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 ticket 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 télé HomeKit

Les accessoires de télécommande télé HomeKit tiers transmettent des événements HID et du son Siri à une Apple TV associée ajoutée à l'aide de l'app Maison. Les événements HID sont envoyés dans le cadre d'une session sécurisée entre l'Apple TV et la télécommande. Une télécommande télé compatible Siri envoie des données audio à l'Apple TV lorsque l'utilisateur active explicitement le micro de la télécommande au moyen d'un bouton dédié à Siri. Les échantillons audio sont envoyés directement à l'Apple TV par le biais d'une connexion réseau locale dédiée entre l'Apple TV et la télécommande. La connexion réseau locale est chiffrée au moyen d'une paire de clés HKDF-SHA-512 dérivées par session, négociée dans le cadre de la session HomeKit entre l'Apple TV et la télécommande télé. HomeKit déchiffre les échantillons audio sur l'Apple TV et les transmet à l'app Siri où ils sont traités avec les mêmes dispositifs de protection de la vie privée que toutes les entrées audio Siri.

SiriKit

Siri utilise le mécanisme d'extension iOS pour communiquer avec les applications tierces. Bien que Siri ait accès aux contacts iOS et à la géolocalisation de l'appareil, Siri vérifie l'autorisation d'accès aux données utilisateur protégées par iOS qui contiennent l'extension pour savoir si l'app a accès avant de lui fournir ces informations. Siri ne passe que le fragment approprié du texte de la requête utilisateur d'origine à l'extension. Par exemple, si l'app n'a pas accès aux contacts iOS, Siri n'interprète pas la relation personnelle dans la requête d'un utilisateur telle que « Envoie 10 euros à ma mère avec <app de paiement> ». Dans ce cas, l'app de l'extension ne voit que « ma mère » à travers le fragment d'occurrence brute qui lui est passé. Cependant, si l'app a effectivement accès aux contacts iOS, elle reçoit les données de contact iOS pour la mère de l'utilisateur. Si un contact a été mentionné dans le corps d'un message, par exemple « Dis à ma mère sur <app de messagerie> que mon frère est génial », Siri n'interprète alors pas « mon frère » indépendamment des termes TCC (Transparency, Consent, and Control) de l'app. Il se peut que le contenu présenté par l'app soit envoyé au serveur pour permettre à Siri de comprendre le vocabulaire qu'un utilisateur est susceptible d'employer dans l'app.
Dans les cas tels que « Dépose-moi chez ma mère en utilisant <nom de l'app> », où la requête de l'utilisateur requiert des informations de géolocalisation issues des contacts de l'utilisateur, Siri fournit des informations sur le lieu à l'extension de l'app, pour cette requête uniquement, indépendamment de la géolocalisation de l'app ou de l'accès aux contacts.

Lors de l'exécution, Siri permet à l'app activée par SiriKit de fournir un ensemble de mots personnalisés propres à l'instance d'application. Ces mots personnalisés sont liés à l'identifiant aléatoire, abordé dans la section Siri de ce document, et possèdent la même durée de vie.

HealthKit

HealthKit stocke et recueille les données provenant des apps de santé et de condition physique avec la permission de l'utilisateur. HealthKit fonctionne également directement avec les appareils de santé et de condition physique, comme les ceintures cardiaques Bluetooth Low Energy (BLE) compatibles et le coprocesseur de mouvement intégré à de nombreux appareils iOS.

Données de santé

HealthKit permet aux utilisateurs de stocker et d'agréger leurs données de santé à partir de sources telles que des apps, des appareils et des établissements de santé. Ces données sont stockées dans la classe de protection des données Protected Unless Open. L'accès aux données est abandonné 10 minutes après le verrouillage de l'appareil et les données redeviennent accessibles la prochaine fois que l'utilisateur saisit son code de verrouillage ou utilise Touch ID ou Face ID pour déverrouiller l'appareil.

HealthKit recueille 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 avec la classe Protected Until First User Authentication.

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 Protected Unless Open. 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 dans iCloud. Lorsqu'elles sont configurées pour le stockage sur iCloud, les données relatives à la santé sont synchronisées entre les appareils et sécurisées par chiffrement qui les protège, que ce soit en transfert ou au repos (at rest). Les données de santé sont uniquement incluses dans les sauvegardes iTunes chiffrées. Elles ne sont incluses ni dans les sauvegardes iTunes non chiffrées, ni dans la sauvegarde iCloud.

Dossiers médicaux

Les utilisateurs ont la possibilité de se connecter à des systèmes de santé compatibles dans l'app Santé pour obtenir leur dossier médical. Lorsqu'il se connecte à un système de santé, l'utilisateur s'authentifie à l'aide d'informations d'identification cliente OAuth 2. Après la connexion, les données du dossier médical sont téléchargées directement depuis l'établissement de santé à travers une connexion protégée par TLS v1.2. Une fois téléchargés, les dossiers médicaux sont stockés de manière sécurisée avec les autres données de 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 tierces

L'accès à l'API HealthKit est contrôlé par des droits (entitlements), 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 renseigner une fiche médicale contenant 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 No Protection afin d'être accessibles sans avoir à saisir le code de verrouillage de l'appareil. La fiche médicale est une fonctionnalité facultative qui permet aux utilisateurs de trouver un juste équilibre entre sécurité et confidentialité. Ces données sont sauvegardées dans Sauvegarde iCloud et ne sont pas synchronisées entre les appareils via CloudKit.

ReplayKit

ReplayKit constitue un framework qui permet aux développeurs d'ajouter des fonctionnalités d'enregistrement et de diffusion en direct à leurs apps. De plus, il permet aux utilisateurs d'annoter leurs enregistrements et leurs diffusions à l'aide de la caméra frontale et du micro de l'appareil.

Enregistrement vidéo

Il existe plusieurs couches de sécurité intégrées à l'enregistrement d'une séquence :

- **Zone de dialogue Autorisations :** avant que l'enregistrement ne démarre, ReplayKit demande à l'utilisateur de reconnaître son intention d'enregistrer l'écran ou d'utiliser le micro ou la caméra frontale. Cette alerte s'affiche une fois par processus d'app et réapparaît si l'app s'exécute en arrière-plan plus de 8 minutes.
- **Capture d'écran et audio :** la capture d'écran et audio se produit hors du processus de l'app dans le daemon *replayd* de ReplayKit. Cela permet de s'assurer que le contenu enregistré n'est jamais accessible au processus de l'app.
- **Création et stockage de film :** le fichier vidéo est écrit dans le répertoire uniquement accessible par les sous-systèmes ReplayKit et jamais à aucune autre app. Cela permet d'éviter que des tiers exploitent les enregistrements sans le consentement de l'utilisateur.
- **Aperçu et partage par l'utilisateur final :** l'utilisateur a la possibilité de prévisualiser et de partager la séquence à travers l'interface utilisateur proposée par ReplayKit. L'interface utilisateur est présentée hors-processus à travers l'infrastructure d'extension iOS et a accès au fichier de séquence généré.

Diffusion

- **Capture d'écran et audio :** le mécanisme de capture d'écran et audio lors de la diffusion est identique à l'enregistrement de séquence et se produit dans *replayd*.
- **Extensions de diffusion :** pour que les services tiers participent à la diffusion ReplayKit, ils doivent créer deux extensions configurées à l'aide du point d'arrivée (endpoint) com.apple.broadcast-services :
  - une extension d'interface utilisateur qui permet à l'utilisateur de configurer sa diffusion ;
  - une extension de transfert qui gère le téléchargement des données vidéo et audio aux serveurs d'arrière-plan (backend) du service.

L'architecture permet de s'assurer que les apps d'hébergement ne possèdent aucun privilège sur le contenu vidéo et audio diffusé — seules les extensions de diffusion ReplayKit et tiers y ont accès.

- **Sélecteur de diffusion :** pour sélectionner le service de diffusion à utiliser, ReplayKit propose un contrôleur de présentation (semblable à UIActivityViewController) que le développeur peut présenter dans son app. Le contrôleur de présentation est implémenté à l'aide du SPI UIRemoteViewController et constitue une extension qui intègre le framework ReplayKit. Il se trouve hors-processus par rapport à l'app hôte.
- **Sélecteur de diffusion système :** permet aux utilisateurs de lancer une diffusion système directement à partir de l'app en utilisant l'interface utilisateur définie par le système et accessible à travers le Centre de contrôle. L'interface utilisateur est implémentée à l'aide du SPI UIRemoteViewController et constitue une extension qui intègre le framework ReplayKit. Elle se trouve hors-processus par rapport à l'app hôte.
- **Extension de téléchargement :** l'extension de téléchargement, que les services de diffusion tiers mettent en place pour gérer le contenu vidéo et audio lors de la diffusion, dispose de deux façons pour recevoir du contenu :
  - en petites séquences MP4 encodées ;
  - en tampons d'échantillons non encodés au format Raw.
    - **Gestion de séquences MP4 :** avec ce mode de gestion, les petites séquences MP4 encodées sont générées par *replayd* et stockées dans un emplacement privé uniquement accessible aux sous-systèmes de ReplayKit. Une fois qu'une séquence est générée, *replayd* communique l'emplacement de cette séquence à l'extension de téléchargement tiers à travers le SPI de la requête NSExtension (s'appuyant sur XPC). *replayd* génère aussi un jeton d'environnement « sandbox » à usage unique également passé à l'extension de téléchargement, ce qui accorde l'accès de l'extension au plan vidéo particulier au cours de la requête d'extension.
    - **Gestion de tampon d'échantillon :** dans ce mode de gestion, les données vidéo et audio sont sérialisées et transmises en temps réel à l'extension de téléchargement tiers à travers une connexion XPC directe. Les données vidéo sont encodées en extrayant l'objet IOSurface du tampon d'échantillon vidéo, de façon sécurisée sous forme d'objet XPC, en les envoyant à travers XPC à l'extension tierce, puis en les redécodant de façon sécurisée dans l'objet IOSurface.

Notes sécurisées

L'app Notes comprend une fonctionnalité de notes sécurisées permettant aux utilisateurs de protéger le contenu de notes spécifiques. 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 entrées sont créées dans Core Data et CloudKit pour stocker les note, mot-clé et vecteur d'initialisation chiffrés, puis les entrées de note d'origine sont supprimées ; les données chiffrées ne sont pas écrites directement. Les pièces jointes sont également chiffrées de cette façon. Parmi les pièces jointes prises en charge, l'on retrouve les images, les dessins, les tableaux, les plans et les sites web. Les notes contenant d'autres types de pièces jointes ne peuvent pas être chiffrées ; 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, ou à passer par 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 de sécurisation est fermée dans les cas suivants :

- l'utilisateur appuie sur le bouton Verrouiller dans Notes ;
- Notes passe en arrière-plan pendant plus de 3 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 celle 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 néanmoins 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 des données chiffrées de type CloudKit pour tout texte ou pièce jointe que l'utilisateur place dans une note. Les actifs sont systématiquement chiffrés à l'aide d'une clé qui est chiffrée dans le CKRecord. Les métadonnées, telles que les dates de création et de modification, ne sont pas chiffrées. CloudKit gère le processus par lequel les participants peuvent chiffrer/déchiffrer les données de chacun.

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 verrouillage de l'utilisateur est également combiné à l'UID de l'appareil pour créer les clés de chiffrement.

Le jumelage de l'Apple Watch avec l'iPhone est sécurisé à l'aide d'un processus hors bande (OOB) pour l'échange des clés publiques, puis à l'aide du secret partagé de la liaison Bluetooth Low Energy (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 BLE standard est employée comme méthode de jumelage de secours, si nécessaire.

Une fois que la session Bluetooth Low Energy est établie et chiffrée en utilisant le protocole de sécurité le plus élevé disponible dans la spécification Bluetooth Core Specification, l'Apple Watch et l'iPhone s'échangent des clés en faisant appel à un processus adapté du service d'identité Apple (IDS) conformément à la description fournie dans la partie « iMessage » de 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 mobiles chiffrées assurant une seconde couche de chiffrement. L'adresse Bluetooth Low Energy est remplacée toutes les 15 minutes pour réduire le risque d'altération du trafic.

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

L'Apple Watch implémente le chiffrement matériel du stockage et la protection des fichiers ainsi que les éléments de trousseau basée sur des classes, comme décrit 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 les communications entre l'Apple Watch et l'iPhone sont aussi sécurisées à l'aide d'une protection basée sur des clés de classe.

Lorsque l'Apple Watch ne se trouve pas dans le champ Bluetooth, la connexion Wi-Fi ou mobile peut être utilisée à la place. L'Apple Watch se connecte automatiquement aux réseaux Wi-Fi auxquels l'iPhone associé s'est déjà connecté et dont les informations d'identification ont été synchronisées avec l'Apple Watch lorsque les deux appareils étaient à portée l'un de l'autre. Ce comportement de connexion automatique peut

ensuite être configuré pour chaque réseau dans la section Wi-Fi de l'app Réglages de l'Apple Watch. Il est possible de se connecter manuellement, via la section Wi-Fi de l'app Réglages de l'Apple Watch, aux réseaux Wi-Fi auxquels aucun des deux appareils ne s'est connecté.

Si l'Apple Watch et l'iPhone sont hors de portée, l'Apple Watch se connecte directement aux serveurs iCloud et Gmail pour récupérer le courrier, au lieu de synchroniser les données de courrier avec l'iPhone associé via Internet. 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 obtenu de Google est ensuite envoyé en format chiffré à l'Apple Watch à travers le service d'identité Apple (IDS) afin qu'il puisse être utilisé pour récupérer le courrier. Ce jeton OAuth n'est jamais utilisé pour les connexions au serveur Gmail à partir de l'iPhone associé.

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 se verrouille automatiquement peu après son retrait du poignet. Lorsque l'Apple Watch est verrouillée, Apple Pay ne peut être utilisé qu'après avoir saisi le code de verrouillage de la montre. La détection du poignet peut être désactivée à l'aide de l'app Apple Watch sur l'iPhone. Ce paramètre peut également être appliqué en utilisant une solution MDM.

L'iPhone jumelé peut aussi déverrouiller l'Apple Watch, à condition que celle-ci soit portée. Ce déverrouillage se fait en établissant 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 verrouillage 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 peut être jumelée uniquement avec un iPhone à la fois. Ce dernier communique les instructions pour effacer tout le contenu et les données de l'Apple Watch lors du déjumelage.

L'Apple Watch peut être configurée pour une mise à jour du logiciel système la prochaine nuit. Pour en savoir plus sur la manière dont le code de verrouillage de l'Apple Watch est stocké afin d'être utilisé durant la mise à jour, consultez la section Conteneurs de clés de ce 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 et depuis un appareil iOS.

Les utilisateurs mobiles doivent pouvoir accéder aux réseaux d'entreprise depuis 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 (et permet aux développeurs d'accéder à) des protocoles de mise en réseau standard pour établir des communications authentifiées, autorisées et chiffrées. Pour atteindre ces objectifs de sécurité, iOS intègre des technologies éprouvées et les dernières normes pour les connexions aux réseaux de données Wi-Fi et mobiles.

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 Transport Layer Security (TLS 1.0, TLS 1.1, TLS 1.2) et DTLS. Il prend en charge AES-128 et AES-256 et privilégie les suites de chiffrement avec PFS (Perfect Forward Secrecy). 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 granulaire. L'API CFNetwork n'autorise pas SSLv3. Les apps qui exploitent WebKit (comme Safari) se voient interdire d'établir une connexion SSLv3.

Dans iOS 11 ou ultérieur et macOS High Sierra ou ultérieur, les certificats SHA-1 ne sont plus autorisés pour les connexions TLS sauf si l'utilisateur les juge fiables. Les certificats dotés de clés RSA qui sont inférieures à 2048 bits sont également interdits. La suite de chiffrement symétrique RC4 est obsolète dans iOS 10 et macOS Sierra. Par défaut, les clients ou serveurs TLS implémentés à travers les API SecureTransport n'ont pas les suites de chiffrement RC4 activées et ne sont pas en mesure de se connecter lorsque RC4 est la seule suite de chiffrement disponible. Pour mieux se sécuriser, les services ou apps qui nécessitent RC4 doivent être mis à niveau pour utiliser les suites modernes et plus sécurisées de chiffrement. Dans iOS 12.1, les certificats émis après le 15 octobre 2018 à partir d'un certificat racine de confiance système doivent être consignés dans un journal « Transparence du certificat » fiable pour que des connexions TLS leurs soient accordées.

App Transport Security

La sécurité du transport des données 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 en cas d'usage des API NSURLConnection, CFURL ou NSURLSession. Par défaut, la sécurité du transport des apps limite la sélection de chiffrement pour n'inclure que les suites qui assurent la confidentialité persistante, particulièrement ECDHE_ECDSA_AES et ECDHE_RSA_AES en mode GCM ou CBC. Les apps sont en mesure de désactiver l'exigence de confidentialité persistante par domaine, auquel cas RSA_AES est ajouté à l'ensemble des chiffrements disponibles.

Les serveurs doivent prendre en charge TLS 1.2 et la confidentialité persistante, et les certificats doivent être valides et signés par l'algorithme SHA-256 ou plus évolué avec une clé RSA sur 2048 bits ou une clé elliptique de 256 bits minimum.

Les connexions réseau ne satisfaisant pas ces critères échouent, à moins que l'app outrepasse l'App Transport Security. L'utilisation de certificats non valides provoque toujours un échec de connection. La sécurité du transport des apps est automatiquement appliquée aux applications compilées pour iOS 9 ou ultérieur.

VPN

Les services réseaux sécurisés, tels que les réseaux privés virtuels, ne nécessitent généralement qu'une configuration minime pour fonctionner avec des 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 cliente appropriée disponible dans 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 ce qui suit :

- Le VPN à la demande pour les réseaux qui utilisent une authentification par certificat. Les services informatiques spécifient les domaines qui nécessitent une connexion VPN à l'aide d'un profil de configuration VPN.
- La fonctionnalité VPN par app permet de définir beaucoup plus finement quand une connexion VPN doit être établie. MDM peut spécifier une connexion pour chaque app gérée et des domaines précis dans Safari. Cela permet de garantir que les données confidentielles sont toujours transmises vers et depuis le réseau de l'entreprise, mais pas les données personnelles d'un utilisateur.
- Le **VPN permanent** peut être configuré pour les appareils gérés via une solution de gestion d'appareils mobiles (MDM) 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 mobiles 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 vers et depuis 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 par le biais 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.

Outre la protection des données, iOS étend la protection de niveau WPA2 aux images de la gestion monodiffusion et multidiffusion à travers le service image de gestion protégée mentionnée dans la norme 802.11w. La prise en charge PMF est disponible sur l'iPhone 6 et l'iPad Air 2 ou ultérieurs.

iOS utilise une adresse MAC (Media Access Control) randomisée lors des recherches Wi-Fi s'il n'est pas déjà associé à un réseau Wi-Fi. Ces recherches sont possibles afin de pouvoir retrouver et connecter un réseau Wi-Fi préféré ou afin d'assister le service de localisation pour les apps exploitant des périmètres géographiques (geofences), par exemple les rappels géodépendants ou la résolution d'un emplacement dans Plans Apple. Il est important de noter que les recherches Wi-Fi qui se produisent lors de la tentative de connexion à un réseau Wi-Fi préféré n'utilisent pas une adresse MAC aléatoire.

iOS utilise également une adresse MAC randomisée pour effectuer des recherches ePNO (enhanced Preferred Network Offload) lorsqu'un appareil n'est pas associé à un réseau Wi-Fi ou que son processeur est en veille. Ces recherches ePNO sont exécutées si un appareil fait appel au service de localisation pour des apps utilisant les périmètres géographiques, comme les rappels en fonction du lieu qui interviennent 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 mobile. Apple a informé les fabricants de cartes Wi-Fi que les recherches Wi-Fi d'iOS utilisent une adresse MAC randomisée, et que ni Apple, ni les fabricants ne peuvent prédire ces adresses MAC randomisées. La prise en charge de la randomisation d'adresse MAC Wi-Fi est indisponible sur l'iPhone 4s et les modèles antérieurs.

Sur l'iPhone 6s ou ultérieur, la propriété masquée d'un réseau Wi-Fi est connue et actualisée automatiquement. Si le Service Set IDentifier (SSID) d'un réseau Wi-Fi est diffusé, l'appareil iOS n'envoie pas de sonde avec le SSID inclus dans la requête. Cela 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 dont Wi-Fi et la bande de base, disposent d'un accès limité à la mémoire du processeur d'application. Lorsqu'une interface USB ou SDIO est utilisée pour interagir avec le processeur réseau, ce dernier ne peut envoyer de transactions d'accès direct à la mémoire (DMA) au processeur d'application. Lorsqu'une interface PCIe est utilisée, chaque processeur réseau se trouve sur son propre bus PCIe isolé. Un IOMMU sur chaque bus PCIe limite l'accès DMA du processeur d'application aux pages de la mémoire contenant ses paquets réseau ou 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 :

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

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

Pour en savoir plus, consultez la page suivante :
https://support.apple.com/ht3647

Authentification unique

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

La SSO iOS fait appel à des jetons SPNEGO et au protocole HTTP Negotiate pour fonctionner avec les services d'authentification basée sur Kerberos et les systèmes d'authentification intégrée Windows prenant en charge les tickets Kerberos. La prise en charge de la SSO repose sur le projet open source Heimdal.

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 la SSO et les applications tierces qui utilisent les API de mise en réseau standard d'iOS peuvent également être configurées pour l'utiliser. Pour configurer la SSO, iOS prend en charge une entité de profil de configuration permettant aux solutions MDM de transmettre les réglages nécessaires. Cela comprend la définition du « User Principal Name » (c'est-à-dire, le compte utilisateur Active Directory) et des réglages du royaume Kerberos, ainsi que la configuration des apps et des URL Safari autorisées à utiliser la SSO.

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, de passer et de recevoir des appels téléphoniques, d'envoyer et de recevoir des messages texte et de partager une connexion Internet mobile.

Handoff

Avec Handoff, l'utilisateur peut placer son ordinateur Mac à côté d'appareils iOS pour transférer automatiquement ce sur quoi il est en train de travailler d'un appareil à l'autre. Handoff permet ainsi à l'utilisateur de passer d'un appareil à l'autre tout en poursuivant son travail 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 via 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 annonces 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 les attaques par réexécution.

La première fois qu'un appareil reçoit une annonce provenant d'une nouvelle clé, il établit une connexion Bluetooth Low Energy à l'appareil émetteur et exécute une annonce d'échange de clés de chiffrement d'annonce. Cette connexion est sécurisée au moyen d'un chiffrement Bluetooth Low Energy 4.2 standard et d'un chiffrement des différents messages (comme dans iMessage). Dans certains cas, ces messages sont transférés à travers les APN plutôt que par Bluetooth Low Energy (BLE). 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 son 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 destiné aux identifications web partagées. Pour en savoir plus à ce sujet, reportez-vous à « Accès aux mots de passe enregistrés par app » dans la section « Chiffrement et protection des données » de ce 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 fonction Handoff d'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 web dans les octets d’annonce Handoff chiffrés. Seuls les autres appareils de l’utilisateur sont capables de déchiffrer les octets d’annonce (tel que décrit précédemment dans cette section).

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 fonction Handoff 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.

Handoff sur des 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 point à point créée par Apple (de la même manière qu’avec AirDrop). L’app Mail, par exemple, utilise ces API pour prendre en charge la fonction Handoff de brouillons de message susceptibles d’inclure des pièces jointes volumineuses.

Lorsqu’une app utilise cette fonctionalité, 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 universel s’appuie sur Handoff pour transférer de façon sécurisée le contenu du presse-papiers d’un utilisateur entre appareils afin de pouvoir copier sur un appareil et coller sur un autre. Le contenu est protégé de façon identique à toute autre donnée Handoff et partagé par défaut avec le presse-papiers universel, à moins que le développeur de l’app ne choisisse de ne pas autoriser le partage.

Les apps ont accès aux données du presse-papiers indépendamment du collage du presse-papiers dans l’app par l’utilisateur. Avec le presse-papiers universel, l’accès à ces données s’étend aux apps en cours d’exécution sur les autres appareils de l’utilisateur (comme établi par sa session iCloud).

Verrouillage automatique

Les ordinateurs Mac prenant en charge le déverrouillage automatique font appel à la technologie Bluetooth Low Energy et aux réseaux Wi-Fi point à point pour autoriser de façon sécurisée l'Apple Watch de l'utilisateur à déverrouiller le Mac. Chaque Mac compatible et Apple Watch associés à un compte iCloud doivent utiliser l'identification à deux facteurs (TFA).

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 aléatoirement un secret de déverrouillage à usage unique, puis le transmet à l'Apple Watch à travers la liaison. Le secret est stocké sur l'Apple Watch et n'est accessible que lorsque l'Apple Watch est déverrouillée (reportez-vous à la partie intitulée « 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.

Au cours d'une opération de déverrouillage, le Mac utilise la technologie Bluetooth Low Energy pour créer une connexion avec l'Apple Watch. Une liaison sécurisée est ensuite établie entre les deux appareils en utilisant les clés partagées générées au moment de la première activation. Le Mac et l'Apple Watch exploitent ensuite un réseau Wi-Fi point à point et une clé sécurisée dérivée de la liaison sécurisée pour déterminer la distance entre les deux appareils. Si les appareils se trouvent dans le champ de détection, la liaison sécurisée est alors utilisée pour transférer le secret prépartagé pour déverrouiller le Mac. Une fois le déverrouillage correctement établi, le Mac remplace le secret de déverrouillage en vigueur par un nouveau secret de déverrouillage à usage unique et le transmet à l'Apple Watch à travers la liaison.

Relais des appels de l'iPhone

Lorsque le Mac, l'iPad ou l'iPod touch d'un utilisateur se trouve sur le même réseau Wi-Fi que son iPhone, ces appareils peuvent passer et recevoir des appels téléphoniques en utilisant la connexion mobile de l'iPhone. Ces appareils doivent pour cela être connectés à la fois à iCloud et à FaceTime à l'aide du même identifiant Apple.

À la réception d'un appel, tous les appareils configurés sont notifiés par l'intermédiaire du **service APN (Apple Push Notification)**, 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 automatiquement transmis depuis l'iPhone de l'utilisateur via une connexion point à point sécurisée entre les deux appareils.

Si un appel est pris sur un appareil, la sonnerie sur les appareils à proximité jumelés à travers iCloud est coupée par le biais d'une brève publication Bluetooth Low Energy. Les octets de cette publication sont chiffrés par le biais de la même méthode que les publications de type Handoff.

Les appels sortants sont également relayés vers l'iPhone par l'intermédiaire du service Apple de notification Push et le son est diffusé de la même manière via la liaison point à point sécurisée entre les appareils.

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

Transfert des SMS de l'iPhone

Le transfert des SMS envoie automatiquement les SMS reçus sur un iPhone à l'iPad, l'iPod touch ou le Mac enregistré de l'utilisateur. Chaque appareil doit être connecté au service iMessage à l'aide du même identifiant Apple. Lorsque le transfert des SMS est activé, l'enregistrement est automatique sur les appareils se trouvant dans le cercle de confiance d'un utilisateur, si l'identification à deux facteurs est activée. Dans le cas contraire, l'enregistrement est vérifié sur chaque appareil en saisissant un code numérique aléatoire à six chiffres généré par l'iPhone.

Une fois les appareils reliés, l'iPhone chiffre et transfère les SMS entrants à chaque appareil en faisant appel aux méthodes décrites dans la partie intitulée « iMessage » de cette 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 SMS en utilisant le mécanisme de transmission de SMS de l'opérateur. Le transfert des SMS peut être activé ou désactivé dans les réglages Messages.

Instant Hotspot

Les appareils iOS prenant en charge Instant Hotspot utilisent Bluetooth Low Energy pour détecter, et communiquer avec, les appareils connectés au même compte iCloud. Les ordinateurs Mac compatibles, exécutant OS X Yosemite ou ultérieur, 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 diffuse 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 à travers 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 point à point créée par Apple pour envoyer des fichiers et des informations aux appareils se trouvant à proximité, notamment les ordinateurs Mac compatibles AirDrop exécutant OS X 10.11 ou ultérieur. Les appareils communiquent directement entre eux par Wi-Fi sans utiliser de connexion Internet ni de point d'accès Wi-Fi.

Lorsqu'un utilisateur active AirDrop, une identité RSA à 2 048 bits est stockée sur l'appareil. Un hachage d'identité AirDrop est en outre 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 émet un signal AirDrop via Bluetooth faible énergie. Les autres appareils allumés et situés à proximité, sur lesquels AirDrop est activé, détectent ce signal et répondent en envoyant une version abrégée du hachage d'identité de leur propriétaire.

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, les hachages d'identité reçus sont comparés à ceux des personnes présentes dans l'app Contacts de l'initiateur. Si une correspondance est trouvée, l'appareil émetteur crée un réseau Wi-Fi point à point et annonce une connexion AirDrop à l'aide de Bonjour. Les appareils récepteurs utilisent alors cette connexion pour envoyer leur hachage d'identité complet à l'initiateur. Si le hachage complet correspond toujours à celui présent dans Contacts, le prénom et la photo du destinataire (si disponibles dans Contacts) s'affichent dans la feuille de partage AirDrop.

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 les certificats d'identité iCloud des deux appareils sont échangés. 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 en provenance de la personne ou de l'appareil identifié. 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 en utilisant une solution MDM.

Partage du mot de passe Wi-Fi

Les appareils iOS qui prennent en charge le partage du mot de passe Wi-Fi, utilisent un mécanisme similaire à AirDrop pour envoyer un mot de passe Wi-Fi d'un appareil à l'autre.

Lorsqu'un utilisateur (le demandeur) sélectionne un réseau Wi-Fi et est invité à saisir le mot de passe correspondant, l'appareil Apple lance une annonce Bluetooth Low Energy indiquant qu'il souhaite le mot de passe Wi-Fi. Les autres appareils Apple en fonctionnement à proximité et qui disposent du mot de passe du réseau Wi-Fi sélectionné se connectent par Bluetooth Low Energy à l'appareil demandeur.

L'appareil disposant du mot de passe Wi-Fi (le cédant) nécessite les coordonnées du demandeur et le demandeur doit prouver son identité en utilisant un mécanisme similaire à AirDrop. Une fois l'identité prouvée, 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 le partage des mots de passe Wi-Fi aux appareils ou apps gérés à l'aide d'une solution MDM.

Apple Pay

Grâce à Apple Pay, les utilisateurs peuvent utiliser leurs appareils compatibles iOS, Apple Watch et Mac pour effectuer en toute simplicité des paiements de façon sûre et confidentielle dans les magasins, les apps et sur le web à travers le navigateur Safari. Les utilisateurs peuvent également ajouter des cartes de transport compatibles Apple Pay à Wallet. Ce système est simple pour les utilisateurs et sécurisé à la fois au niveau du matériel et des logiciels.

Apple Pay est aussi conçu pour protéger les informations personnelles de l'utilisateur. Apple Pay 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 : Secure Element est une puce certifiée standard exécutant la plateforme Java Card, qui est conforme 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 Secure Element, et entre Secure Element et le terminal de point de vente.

Wallet : Wallet permet d'ajouter et de gérer des cartes bancaires, de crédit et de fidélité, et de réaliser des paiements avec Apple Pay. Les utilisateurs peuvent consulter leurs cartes et, dans certains cas, afficher des informations supplémentaires fournies par l'émetteur de leur carte, comme la politique de confidentialité de celui-ci, les transactions récentes ou d'autres renseignements dans Wallet. Ils peuvent également ajouter des cartes à Apple Pay dans :

- Assistant réglages et Réglages pour iOS ;
- l'app Watch pour Apple Watch ;
- la sous-fenêtre Wallet et Apple Pay des Préférences Système pour Mac.

De plus, Wallet permet aux utilisateurs d'ajouter des cartes de transport, des cartes de fidélité, des cartes d'embarquement, des tickets, des cartes cadeaux, des cartes d'étudiant, etc., afin de les gérer.

Secure Enclave : sur l'iPhone, l'iPad et l'Apple Watch, Secure Enclave gère le processus d'authentification et permet à une opération de paiement de se réaliser.

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 à Secure Element ou Secure Enclave le cas échéant, directement sans passer par le processeur d'application.

Serveurs Apple Pay : les serveurs Apple Pay gèrent la configuration et la mise à disposition des cartes bancaires, cartes de transport et cartes d'étudiant dans Wallet, ainsi que les numéros de compte d'appareil stockés dans 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 accréditations pour les paiements réalisés dans les apps.

Comment Apple Pay utilise Secure Element

Secure Element renferme un « applet » spécifiquement conçu pour gérer Apple Pay. Il comprend également des applets certifiés par des réseaux de paiement ou des émetteurs de cartes. Le réseau de paiement ou l'émetteur de la carte transmet sous forme chiffrée les données des cartes bancaires ou prépayées à ces applets 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 ces applets et protégées à l'aide des fonctionnalités de sécurité de Secure Element. Lors d'une transaction, le terminal communique directement avec Secure Element via le contrôleur de communication en champ proche (NFC) par le biais d'un bus matériel dédié.

Comment Apple Pay utilise le contrôleur NFC

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

Une fois qu'un paiement par carte bancaire ou carte prépayée (y compris carte de fidélité) est autorisé par le détenteur de la carte à l'aide de Touch ID, de Face ID ou d'un code de verrouillage, ou par un double-clic sur le bouton latéral sur une Apple Watch déverrouillée, les réponses sans contact préparées par les applets de paiement dans Secure Element sont acheminées par le contrôleur exclusivement vers le champ NFC. Les détails d'autorisation de paiement des transactions de paiement sans contact sont donc transmis uniquement au champ NFC local et ne sont jamais divulgués au processeur d'application. Cependant, pour les paiements réalisés dans les apps et sur le web, ces détails sont acheminés vers le processeur d'application, mais uniquement après chiffrement par Secure Element vers le serveur Apple Pay.

Transfert sur cartes bancaires et prépayées

Lorsqu'un utilisateur ajoute une carte bancaire ou prépayée (y compris une carte de fidélité) 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 concerné ou à son fournisseur de service agréé. 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 1.2.

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 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 bancaire 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 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 à Apple Pay à l'aide de l'app Apple Watch sur l'iPhone ou dans l'app iPhone de l'émetteur de carte. 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 Secure Element sur l'Apple Watch.

Lorsque des cartes bancaires ou prépayées (y compris des cartes de fidélité) sont ajoutées, elles apparaissent dans une liste de cartes affichée dans l'Assistant réglages sur les appareils connectés au même compte iCloud. Ces cartes demeurent dans cette liste tant qu'elles sont actives sur au moins un des appareils. Elles sont retirées de cette liste une fois qu'elles ont été supprimées de tous les appareils pendant sept jours. Cette fonction nécessite l'activation de l'identification à deux facteurs sur le compte iCloud concerné.

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 depuis Réglages, l'app Wallet ou l'app de l'Apple Watch, ou à l'aide de l'objectif de l'appareil. Lorsque la caméra capture les informations de la carte, Apple tente de renseigner le nom, le numéro de carte et la date d'expiration. La photo n'est jamais enregistrée sur l'appareil ni stockée dans la photothèque. Une fois tous les champs renseignés, le processus de vérification de carte valide 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 conditions générales, Apple télécharge les conditions générales de l'émetteur de la carte concerné et les présente à l'utilisateur. Si ce dernier accepte les conditions générales, Apple envoie l'identifiant des conditions 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 lier la carte à Secure Element.

Le fichier de ticket 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 ticket qui comprend des informations indiquant par exemple si la personnalisation de 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 d'une carte bancaire à Apple Pay à partir d'un compte iTunes Store

Pour les cartes bancaires dans iTunes, l'utilisateur est parfois invité à saisir à nouveau son mot de passe d'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 conditions d'utilisation, puis les envoie avec l'identifiant des conditions et le code de sécurité de la carte au processus de liaison et transfert. Une vérification supplémentaire peut être effectuée pour les cartes liées à un compte iTunes.

Ajout d'une carte bancaire depuis l'app d'un émetteur de carte

Lorsque l'app est inscrite pour être utilisée avec Apple Pay, des 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, décrit ci-dessous, hormis que des mots de passe à usage unique sont utilisés au lieu de 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 SMS, un e-mail, un appel au service client ou une procédure intégrée à une app tierce agréée. Pour la vérification par SMS 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 l'app Apple Watch est envoyé. Pour le service client ou la vérification à l'aide d'une app, l'émetteur utilise son propre processus de communication.

Autorisation du paiement

Sur les appareils dotés de Secure Enclave, Secure Element n'autorise le paiement qu'après avoir reçu l'autorisation de Secure Enclave. Sur l'iPhone ou l'iPad, cela suppose la confirmation que l'utilisateur s'est authentifié par Touch ID, Face ID ou le code de verrouillage de l'appareil. Touch ID ou Face ID est la méthode par défaut, si elle est disponible. Cependant, le code de verrouillage peut être utilisé à tout moment. La vérification par code de verrouillage est automatiquement proposée après trois tentatives infructueuses de reconnaissance d'empreinte digitale ou deux tentatives infructueuses de reconnaissance faciale, et devient la seule option possible après la cinquième tentative infructueuse. Un code de verrouillage 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 de verrouillage et l'utilisateur doit appuyer deux fois sur le bouton latéral pour réaliser un paiement.

La communication entre Secure Enclave et Secure Element est effectuée via une interface série, Secure Element étant connecté au contrôleur NFC lui-même connecté au processeur d'application. Bien qu'ils ne soient pas directement connectés, Secure Enclave et 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 utilisées des deux côtés pour assurer la protection contre les attaques par réexécution (« replay attacks »). La clé de jumelage est générée à l'intérieur de Secure Enclave, à partir de sa clé d'identification et de l'identifiant unique de Secure Element. Cette clé de jumelage est ensuite transférée de manière sécurisée en usine depuis Secure Enclave jusqu'à un **module de sécurité matériel (HSM)** qui dispose du matériel nécessaire pour injecter ensuite la clé de jumelage dans Secure Element.

Lorsque l'utilisateur autorise une transaction, Secure Enclave envoie à 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 Secure Enclave lorsqu'un utilisateur transfère pour la première fois une carte bancaire. Elle est conservée tant qu'Apple Pay est activé ; elle est protégée par le chiffrement et le mécanisme anti-rollback de Secure Enclave. Elle est transmise de manière sécurisée à Secure Element par le biais de la clé de jumelage. À la réception d'une nouvelle valeur AR, Secure Element marque toutes les cartes précédemment ajoutées comme supprimées.

Les cartes bancaires et prépayées ajoutées à Secure Element ne peuvent être utilisées que si une autorisation est présentée à 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 à Secure Enclave de rendre des cartes inutilisables en marquant la copie de la valeur AR en sa possession comme invalide dans les cas suivants :

- le code de verrouillage 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 de verrouillage de l'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, Secure Element vérifie l'autorisation envoyée par 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 (code à usage unique) est calculé au moyen d'un compteur de transactions dont la valeur augmente d'une unité à chaque nouvelle transaction, ainsi que d'une clé fournie dans l'applet de paiement durant la personnalisation et connue du réseau de paiement ou de l'émetteur. En fonction du système de paiement, il est possible d'utiliser d'autres données pour le calcul, notamment les données suivantes :

- un nombre imprévisible généré par la borne en cas de transaction NFC ;
- un nonce de serveur Apple Pay dans le cas de transactions effectuées dans des apps.

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 à l'aide de cartes bancaires 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, ce qui est géré 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 équipés de Touch ID ;
- appuyer deux fois sur le bouton latéral des appareils équipés de Face ID.

L'utilisateur doit ensuite s'authentifier via Touch ID, Face ID ou son code de verrouillage pour que les données de paiement soient transmises. Lorsque l'Apple Watch est déverrouillée, un double appui sur le bouton latéral permet d'activer la carte par défaut pour le paiement. Aucune information de paiement n'est envoyée sans authentification de l'utilisateur.

Une fois l'utilisateur 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'envoie 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 Apple.

Paiement à l'aide de cartes bancaires dans les apps

Apple Pay permet aussi d'effectuer des paiements dans des apps iOS et dans des apps Apple Watch. Lorsque des utilisateurs effectuent des paiements depuis 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 ou vendeur avant de les envoyer à ce dernier. Apple Pay conserve des données de transaction anonymes comme le montant approximatif de l'achat. Ces données ne peuvent être associées à un utilisateur spécifique 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 mire 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 via Touch ID, Face ID ou en saisissant le code de verrouillage de l'appareil. Une fois le paiement autorisé, les informations figurant sur la mire 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 transmises à Secure Element afin de générer une accréditation de paiement destinée à être chiffrée à l'aide d'une clé Apple. Lorsque l'accréditation de paiement chiffrée a été générée par Secure Element, elle est transmise aux serveurs Apple Pay qui la déchiffrent, comparent le nonce inclus dans cette accréditation au nonce envoyé initialement 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 à travers 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 un droit spécifiant les identifiants de vendeur pris en charge. Une app peut également inclure des données supplémentaires à envoyer à 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. Cela est réalisé par le développeur de l'app qui peut spécifier 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 à l'aide de cartes bancaires sur le web

Apple Pay peut être utilisé pour effectuer des paiements sur des sites web à partir d'un appareil iOS, d'une Apple Watch ou d'un Mac. Il est possible également de commencer une transaction Apple Pay sur un Mac et de la terminer sur un iPhone ou une Apple Watch compatible Apple Pay par le biais du même compte iCloud.

Apple Pay sur le web oblige tous les sites web participants à s'inscrire auprès d'Apple. Les serveurs d'Apple réalisent la validation du nom de domaine et émettent un certificat client TLS. Les sites web prenant en charge Apple Pay doivent servir leur contenu par HTTPS. Pour chaque transaction de paiement, les sites web doivent obtenir une session vendeur sécurisée et unique à travers un serveur Apple émettant le certificat client TLS. Les données de session vendeur sont signées par Apple. Une fois qu'une signature de session vendeur est vérifiée, un site web peut demander si l'utilisateur possède un appareil compatible Apple Pay et si sa carte bancaire ou prépayée est activée sur cet 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 réglages de confidentialité de Safari sous iOS et macOS.

Une fois qu'une session vendeur est validée, toutes les mesures de sécurité et de confidentialité sont identiques à celles du paiement dans une app.

En cas de Handoff du Mac vers l'iPhone ou l'Apple Watch, Apple Pay utilise le protocole du service d'identité Apple (IDS) chiffré de bout-en-bout pour transmettre les informations liées au paiement entre le Mac de l'utilisateur et l'appareil effectuant l'autorisation. IDS fait appel aux clés de l'appareil de l'utilisateur pour procéder au chiffrement de sorte qu'aucun autre appareil ne puisse déchiffrer ces informations, et les clés ne sont pas visibles par Apple. La découverte d'appareils pour le Handoff Apple Pay contient le type et l'identifiant unique des cartes bancaires de l'utilisateur accompagnés de certaines métadonnées. Le numéro de compte spécifique à l'appareil de la carte de l'utilisateur n'est pas partagé et reste 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 récemment employées par l'utilisateur à travers le trousseau iCloud.

Lorsque l'utilisateur autorise le paiement à l'aide de Touch ID, Face ID ou d'un code de verrouillage, ou effectue un double-clic sur la touche latérale de l'Apple Watch, un jeton de paiement chiffré de façon unique pour chaque certificat de vendeur du site web est transmis de façon sécurisée de l'iPhone ou de l'Apple Watch de l'utilisateur à son Mac, puis livré au site web du vendeur.

Seuls les appareils à proximité l'un de l'autre peuvent demander et effectuer un paiement. La proximité est déterminée par publications Bluetooth Low Energy.

Cartes sans contact

Wallet prend en charge le protocole de service à valeur ajoutée VAS (Value Added Service) pour transmettre les données des cartes prises en charge à des bornes NFC compatibles. Le protocole VAS peut être mis en œuvre sur des bornes sans contact de vendeur et exploite la technologie NFC pour communiquer avec des appareils Apple pris en charge. Le protocole VAS fonctionne sur de courtes distances et peut être utilisé pour présenter des cartes sans contact indépendamment ou dans le cadre d'une transaction Apple Pay.

Lorsque l'appareil est tenu à proximité de la borne NFC, cette dernière lance la réception des données de la carte en envoyant une requête de carte. Si l'utilisateur possède une carte incluant l'identifiant du vendeur, il est invité à autoriser son usage à l'aide de Touch ID, de Face ID ou d'un code de verrouillage. Les informations de la carte, à savoir un horodatage et une clé ECDH P-256 aléatoire à usage unique, sont utilisées avec la clé publique du vendeur pour générer une clé de chiffrement destinée aux données de la carte, lesquelles sont envoyées à la borne.

Les utilisateurs peuvent également sélectionner manuellement une carte et l'autoriser à l'aide de Touch ID, de Face ID ou d'un code de verrouillage avant de la présenter à la borne NFC du vendeur.

Apple Pay Cash

Dans iOS 11.2 ou ultérieur et watchOS 4.2 ou ultérieur, Apple Pay peut être utilisé sur un iPhone, un iPad ou une Apple Watch pour envoyer, recevoir et demander de l'argent à d'autres utilisateurs. Lorsqu'un utilisateur reçoit de l'argent, la somme est ajoutée à son compte Apple Pay Cash accessible depuis Wallet ou en sélectionnant Réglages > Wallet et Apple Pay depuis n'importe quel appareil admissible sur lequel l'utilisateur s'est connecté avec son identifiant Apple.

Pour effectuer des paiements entre particuliers et utiliser Apple Pay Cash, l'utilisateur doit être connecté à son compte iCloud depuis un appareil compatible avec Apple Pay Cash et avoir l'identification à deux facteurs configurée sur son compte iCloud.

Lorsque vous configurez Apple Pay Cash, il se peut que les informations saisies au moment de l'ajout d'une carte bancaire soit partagée avec notre banque partenaire, Green Dot Bank, et avec Apple Payments Inc., une filiale créée pour préserver la confidentialité de vos données en stockant et traitant les informations séparément du reste d'Apple. Ces informations sont utilisées exclusivement à des fins réglementaires, de dépannage et de prévention de la fraude.

Les demandes et les virements d'argent entre les utilisateurs sont engagées depuis l'app Messages ou en demandant à Siri. Lorsqu'un utilisateur essaie d'envoyer de l'argent, iMessage affiche la page Apple Pay. Le solde d'Apple Pay Cash est toujours utilisé en premier. Si nécessaire, des fonds supplémentaires sont débités sur la seconde carte bancaire ajoutée à Wallet par l'utilisateur.

La carte Apple Pay Cash ajoutée dans Wallet peut être utilisée avec Apple Pay pour effectuer des paiements dans des boutiques, des apps et sur Internet. Il est également possible de virer l'argent disponible dans Apple Pay Cash sur un compte bancaire. En plus de recevoir de l'argent d'un autre utilisateur, il est possible d'en ajouter au compte Apple Pay Cash à partir d'une carte bancaire ou prépayée dans Wallet.

Apple Payments Inc. stocke vos transactions et peut les utiliser à des fins de dépannage, de prévention de la fraude et légales une fois une transaction réalisée. Le reste d'Apple ne sait pas à qui vous envoyez de l'argent, de qui vous en recevez ou où vous avez effectué votre achat à l'aide de votre carte Apple Pay Cash.

Lorsque vous envoyez de l'argent par Apple Pay Cash, que vous ajoutez de l'argent à un compte Apple Pay Cash ou que vous transférez de l'argent sur un compte bancaire, un appel aux serveurs Apple Pay est effectué pour obtenir un nonce cryptographique similaire à la valeur renvoyée pour Apple Pay dans les apps. Le nonce ainsi que d'autres données de transaction sont transmis à Secure Element afin de générer une signature de paiement. Lorsque la signature de paiement sort de Secure Element, elle est transmise aux serveurs Apple Pay. L'authentification, l'intégrité et l'exactitude de la transaction sont vérifiées par le biais de la signature de paiement, tandis que le nonce est vérifié par les serveurs Apple Pay. Le transfert d'argent est ensuite lancé et vous êtes averti dès qu'il est terminé.

Si la transaction implique l'utilisation d'une carte bancaire pour ajouter de l'argent à Apple Pay Cash, envoyer de l'argent à un autre utilisateur ou rajouter de l'argent si le solde Apple Pay Cash est insuffisant, une accréditation de paiement chiffrée, semblable à celles qui sont utilisées pour Apple Pay dans les apps et sur les sites web, est alors également générée et envoyée aux serveurs Apple Pay.

Une fois que le solde Apple Pay Cash dépasse un certain montant ou si une activité inhabituelle est détectée, l'utilisateur est invité à vérifier son identité. Les informations fournies pour vérifier l'identité de l'utilisateur, telles que le numéro de sécurité sociale ou les réponses à des questions (pour confirmer le nom d'une rue dans laquelle vous avez vécu dans le passé, par exemple), sont transmises en toute sécurité au partenaire d'Apple et chiffrées en utilisant sa clé. Apple est incapable de déchiffrer ces données.

Cartes de transport

En Chine et au Japon, les utilisateurs peuvent ajouter des cartes de transport prises en charge à Wallet sur les modèles d'iPhone et d'Apple Watch pris en charge. Pour ce faire, il convient soit de transférer le solde et la carte de transport de la carte physique vers son équivalent Wallet numérique, soit d'approvisionner une nouvelle carte de transport dans Wallet depuis l'app de l'émetteur de la carte de transport. Une fois qu'une carte de transport a été ajoutée à Wallet, l'utilisateur peut voyager en présentant simplement son iPhone ou son Apple Watch devant le lecteur de carte de la société de transport. Au Japon, la carte Suica peut également être utilisée pour effectuer des paiements.

Les cartes de transport ajoutées sont associées au compte iCloud de l'utilisateur. Si l'utilisateur ajoute plusieurs cartes à Wallet, Apple ou l'émetteur de la carte de transport peut éventuellement lier les informations personnelles de l'utilisateur et les informations du compte associé entre les cartes. Par exemple, les cartes MySuica peuvent être liées à des cartes Suica anonymes. Les transactions et les cartes de transport 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 les chiffres d'identification du numéro de série de la carte. Il se peut également qu'ils doivent fournir des informations personnelles pour prouver qu'ils sont bien les détenteurs de la carte. Si la carte est une carte MySuica ou une carte Suica qui contient une carte de transport, par exemple, les utilisateurs doivent également saisir leur date de naissance. Lors du transfert d'un iPhone vers une Apple Watch, les deux appareils doivent être en ligne.

Le solde peut être rechargé avec des fonds provenant d'une carte bancaire ou prépayée via Wallet ou depuis l'app de l'émetteur de la carte. La sécurité de la recharge du solde lors de l'utilisation d'Apple Pay est décrite dans la section « Paiement à l'aide de cartes bancaires dans les apps » de ce document.

La procédure qui consiste à transférer la carte de transport depuis l'app de l'émetteur de la carte de transport est décrite dans la section « Ajout d'une carte bancaire depuis l'app d'un émetteur de carte » de ce document.

L'émetteur de la carte de transport dispose des clés cryptographiques nécessaires pour authentifier la carte physique et vérifier les données saisies par l'utilisateur. Une fois vérifiées, le système peut créer un numéro de compte d'appareil pour le Secure Element et activer la carte nouvellement ajoutée dans Wallet avec le solde transféré. Au Japon, une fois le transfert à partir de la carte physique effectué, la carte Suica physique est désactivée.

À la fin du transfert, le solde de la carte de transport est chiffré et stocké dans un applet dédié au sein de Secure Element. L'entreprise de transport dispose des clés pour réaliser des opérations cryptographiques sur les données de la carte pour les transactions.

Les utilisateurs bénéficient, par défaut, de l'intégration d'Express Transit qui leur permet de payer et de voyager sans recourir à Touch ID, Face ID ou un code de verrouillage. Les informations telles que les arrêts récemment fréquentés, l'historique des transactions et les tickets supplémentaires peuvent être consultées par tout lecteur de carte sans contact situé à proximité lorsque le mode Express est activé. Les utilisateurs peuvent activer l'autorisation par Touch ID, Face ID ou un code de verrouillage dans les réglages Wallet et Apple Pay en désactivant Transport express.

Tout comme avec d'autres cartes Apple Pay, les utilisateurs peuvent suspendre ou supprimer les cartes de transport comme suit :

- en effaçant l'appareil à distance à travers Localiser mon iPhone,
- en activant le mode Perdu à travers Localiser mon iPhone,
- en utilisant une commande d'effacement à distance MDM,
- en supprimant toutes les cartes de la page du compte de leur identifiant Apple,
- en supprimant toutes les cartes d'iCloud.com,
- en supprimant toutes les cartes de Wallet,
- en supprimant la carte dans l'app de son émetteur.

Les serveurs Apple Pay informent la société de transport de la nécessité de suspendre ou de désactiver ces cartes. Pour les cartes Suica, si les appareils des utilisateurs sont déconnectés lorsqu'ils essaient de les effacer, il se peut que les cartes Suica restent actives sur certaines bornes jusqu'à 00:01, heure du Japon, le jour suivant. Si les appareils des utilisateurs sont déconnectés, les cartes de transport pourront toujours être utilisées en Chine.

Si les utilisateurs suppriment leurs cartes de transport, il est possible de récupérer le solde en les ajoutant à nouveau à un appareil connecté à l'aide du même identifiant Apple.

Cartes d'étudiant

Sous iOS 12, les étudiants, professeurs et membres du personnel des établissements d'enseignement participants peuvent ajouter leur carte d'identité à Wallet pour accéder à des lieux et payer partout où leur carte est acceptée.

L'utilisateur ajoute sa carte d'identité à Wallet au moyen d'une app fournie par l'émetteur de la carte d'identité ou l'établissement d'enseignement participant. Le processus technique utilisé est le même que celui décrit à la section « Ajout d'une carte bancaire depuis l'app d'un émetteur de carte » plus haut dans ce guide. Les apps de l'émetteur doivent en plus prendre en charge l'identification à deux facteurs sur les comptes qui contrôlent l'accès à leurs identifiants. Il est possible de configurer une carte simultanément sur deux appareils Apple pris en charge et connectés au même identifiant Apple.

Lorsqu'une carte d'étudiant est ajoutée à Wallet, le mode Express est activé par défaut. Les cartes d'étudiant en mode Express interagissent avec les bornes qui les acceptent, sans passer par l'authentification par Touch ID, Face ID ou un code de verrouillage. L'utilisateur peut toucher le bouton Plus à l'avant de la carte d'identité dans Wallet et désactiver le mode Express pour désactiver cette fonction. La réactivation du mode Express nécessite Touch ID, Face ID ou un code de verrouillage.

Il est possible de désactiver ou de supprimer des cartes d'étudiants comme suit :

- en effaçant l'appareil à distance à travers Localiser mon iPhone,
- en activant le mode Perdu à travers Localiser mon iPhone,
- en utilisant une commande d'effacement à distance MDM,
- en supprimant toutes les cartes de la page du compte de leur identifiant Apple,
- en supprimant toutes les cartes d'iCloud.com,
- en supprimant toutes les cartes de Wallet,
- en supprimant la carte dans l'app de son émetteur.

Suspension, retrait et effacement de cartes

Les utilisateurs ont la possibilité de suspendre Apple Pay sur l'iPhone, l'iPad et l'Apple Watch en plaçant leur appareil en mode Perdu à l'aide de la fonctionnalité Localiser mon iPhone. Ils peuvent également retirer et supprimer leurs cartes d'Apple Pay à l'aide de la fonctionnalité Localiser mon iPhone, d'iCloud.com ou directement sur leur appareil à l'aide de Wallet. Sur l'Apple Watch, les cartes peuvent être supprimées à l'aide des réglages iCloud, via l'app Apple Watch sur l'iPhone ou directement sur la montre. La possibilité d'effectuer des paiements en utilisant des cartes sur l'appareil est alors suspendue ou supprimée d'Apple Pay par l'émetteur de la carte ou le réseau de paiement concerné, même si l'appareil n'est pas connecté à un réseau mobile 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 », via Localiser mon iPhone ou en restaurant son appareil en mode de récupération, iOS demande à Secure Element de marquer toutes les cartes comme supprimées. Cela 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, Secure Enclave marque la valeur AR (Authorization Random) comme étant invalide de sorte qu'il ne soit plus possible d'autoriser des paiements avec des cartes précédemment enregistrées. Une fois en ligne, l'appareil essaie de contacter les serveurs Apple Pay pour s'assurer que toutes les cartes présentes dans Secure Element sont effacées.

Services Internet

Création de mots de passe d'identifiant Apple complexes
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, tous les nouveaux comptes doivent contenir les attributs de mot de passe suivants :

- 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, Suggestions Siri, iCloud, Sauvegarde iCloud et Trousseau iCloud.

Ces services Internet ont été développés avec les mêmes objectifs de sécurité que ceux d'iOS mis en avant à travers toute 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

Un Identifiant Apple correspond à un compte utilisé pour se connecter à des services Apple comme iCloud, iMessage, FaceTime, l'iTunes Store, Apple Books, l'App Store 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 ne correspondant à aucun mot de passe utilisé. 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 e-mails et des notifications push 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 règles et de procédures conçues 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 réguliers des règles pour aider Apple à s'adapter à toute nouvelle information susceptible d'affecter la sécurité des clients.

Identification à deux facteurs

Pour aider les utilisateurs à renforcer la sécurité de leur compte, Apple propose *l'identification à deux facteurs*, une couche supplémentaire de sécurité pour les identifiants Apple. Elle est conçue dans le but de s'assurer que seul le propriétaire du compte peut accéder au compte, 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 validation 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'identification à deux facteurs améliore la sécurité de l'Identifiant Apple de l'utilisateur et de l'intégralité des informations confidentielles qu'il confie à Apple pour les stocker. 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'identification à deux facteurs, consultez : https://support.apple.com/HT204915

Validation en deux étapes

Apple propose en outre depuis 2013 un moyen sécurisé similaire appelé validation en deux étapes. Lorsque cette méthode est activée, l'identité de l'utilisateur doit être validée 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, toute connexion à iCloud, à iMessage, à FaceTime et au Game Center, ou avant tout achat sur l'iTunes Store, Apple Books ou l'App Store à partir d'un nouvel appareil. Les utilisateurs disposent également d'une clé de récupération de 14 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. Bien que la plupart des nouveaux utilisateurs soient invités à utiliser l'identification à deux facteurs, il existe toujours des cas où la validation en deux étapes est privilégiée.

Pour en savoir plus sur la validation en deux étapes d'un identifiant Apple, consultez : https://support.apple.com/HT5570

Identifiants Apple gérés

Les identifiants Apple gérés fonctionnent de façon similaire aux 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 par FaceTime et Messages, et configurer des autorisations s'appuyant sur des rôles pour les membres du personnel, les enseignants 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, consultez : 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 enseignant peuvent se voir accorder des privilèges d'audit pour certains identifiants Apple gérés. Les auditeurs sont en mesure de contrôler uniquement les comptes qui se trouvent en dessous 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'identification d'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 app compatibles 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 l'accès, l'heure de la demande et si l'audit a été réalisé.

Pour en savoir plus sur l'audit des identifiants Apple gérés, consultez : https://help.apple.com/schoolmanager/#/tesd8fcbdd99

Identifiants Apple gérés et appareils personnels

Les identifiants Apple gérés peuvent également être utilisés avec des appareils iOS personnels et des ordinateurs Mac. 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'identification 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, comme FaceTime ou Messages. Tout document iCloud créé par des étudiants connectés, est soumis à un audit, comme expliqué plus tôt dans cette section.

iMessage

L'application iMessage d'Apple 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 ni les messages ni les pièces jointes qui sont protégées par un système de chiffrement de bout en bout, afin que personne d'autre que l'expéditeur et le destinataire ne puissent y accéder. Apple est incapable 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 1280 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 d'annuaire. 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 via la carte SIM et le réseau de l'opérateur. Avec certains réseaux, cela nécessite l'usage de SMS (l'utilisateur verra s'afficher une boîte de dialogue de confirmation si le SMS n'est pas évalué à zéro). La vérification du numéro de téléphone peut être requise pour plusieurs services du système en plus d'iMessage, tels que 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 ultérieur, les messages, envoyés à partir de différentes adresses qui sont liées au même identifiant Apple, sont affichés sous forme de conversation unique sur les appareils qui les reçoivent. Ce comportement est facilité par un identifiant de compte récupéré à partir du service IDS avec les clés publiques et les adresses du service APN pour une adresse électronique 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 du service APN via 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 destinataire, l'appareil expéditeur génère une valeur aléatoire sur 88 bits et l'utilise comme clé HMAC-SHA256 pour élaborer une valeur sur 40 bits dérivée de la clé publique de l'expéditeur et du destinataire et du texte en format simple. La concaténation des valeurs 88 bits et 40 bits produit une clé de 128 bits qui permet de chiffrer le message par la méthode AES en mode CTR. La valeur 40 bits est employée par le destinataire pour vérifier l'intégrité du texte au format simple déchiffré. Cette clé AES propre à chaque message est chiffrée via RSA-OAEP avec 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 **URI (Uniform Resource Identifier)** 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 illustration ci-dessous).

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 une durée maximale de 30 jours.

Business Chat

Business Chat est un service de messagerie qui permet aux utilisateurs de communiquer avec des entreprises au moyen de l'app Messages. Seuls les utilisateurs sont autorisés à lancer une conversation ; l'entreprise contactée reçoit un identifiant opaque pour l'utilisateur. L'entreprise ne reçoit ni le numéro de téléphone, ni l'adresse e-mail, ni les données de compte iCloud de l'utilisateur. Lorsque vous discutez avec Apple, l'entreprise reçoit un identifiant Business Chat associé à votre identifiant Apple. Les utilisateurs conservent le contrôle de la communication. La suppression d'une conversation Business Chat entraîne l'effacement de cette conversation dans l'app Messages de l'utilisateur et bloque l'entreprise afin qu'elle ne puisse plus envoyer de messages à cet utilisateur.

Les messages envoyés à l'entreprise sont chiffrés individuellement entre l'appareil de l'utilisateur et les serveurs de messagerie Apple qui déchiffrent ensuite ces messages et les transmettent à l'entreprise via le protocole TLS. Les réponses de l'entreprise sont transmises de la même manière via TLS aux serveurs de messagerie Apple qui chiffrent à nouveau le message avant qu'il ne parvienne à l'appareil de l'utilisateur. Comme avec iMessage, les messages sont mis en file d'attente pendant 30 jours au maximum avant d'être transmis aux appareils déconnectés.

FaceTime

FaceTime est le service d'appels audio et vidéo d'Apple. À l'instar d'iMessage, les appels FaceTime utilisent également le service de notifications Push d'Apple (APN) pour établir une première connexion aux appareils enregistrés de l'utilisateur. Le contenu audio/vidéo 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 est incapable de déchiffrer ces données.

La connexion FaceTime initiale s'établit par le biais de l'infrastructure du serveur Apple qui relaye les paquets de données entre les appareils enregistrés des utilisateurs. Par le biais du service de notifications APN et de messages STUN (Session Traversal Utilities for NAT) sur la connexion relayée, les appareils valident leurs certificats d'identification et établissent un secret partagé pour chaque session. Le secret partagé est utilisé pour dériver les clés de session des chaînes diffusées via le profil de RTP Secure Real-time Transport Protocol (SRTP). Les paquets SRTP sont chiffrés en utilisant AES-256 en Counter Mode et HMAC-SHA1. À la suite de la connexion et de la configuration de sécurité initiales, FaceTime utilise STUN et Internet Connectivity Establishment (ICE) pour établir une connexion point à point entre les appareils, dans la mesure du possible.

FaceTime en groupe étend FaceTime à la prise en charge de groupes jusqu'à 33 participants simultanés. Comme avec les appels FaceTime classiques entre deux interlocuteurs, les appels sont chiffrés de bout-en-bout entre les appareils des participants invités. Si la plupart de l'infrastructure et de la conception des appels FaceTime classiques est réutilisée, les appels FaceTime en groupe se caractérisent par un nouveau mécanisme de génération de clé qui s'appuie sur l'authenticité qu'offre le service IDS. Ce protocole fournit la confidentialité persistante, à savoir l'assurance que l'appareil d'un utilisateur ne fuitera pas le contenu des appels passés. Les clés de session sont enveloppées par AES-SIV et distribuées parmi les participants à l'aide d'une construction ECIES avec des clés P-256 ECDH éphémères.

Lorsqu'un nouveau numéro de téléphone ou une nouvelle adresse e-mail est ajoutée à un appel FaceTime en groupe, les appareils actifs établissent de nouvelles clés multimédias et ne partagent en aucun cas les clés précédemment utilisées avec les nouveaux appareils invités.

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 cet utilisateur. 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 via des profils de configuration MDM. 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.

iCloud divise chaque fichier en plusieurs blocs qu'il chiffre à l'aide de l'algorithme AES-128 et d'une clé SHA-256 dérivée du contenu de chaque bloc. Les clés et les métadonnées du fichier sont stockées par Apple dans le compte iCloud de l'utilisateur. Les parties chiffrées du fichier sont stockées, sans les clés ni toute information susceptible d'identifier l'utilisateur, en faisant appel à des services de stockage Apple et tiers.

iCloud Drive

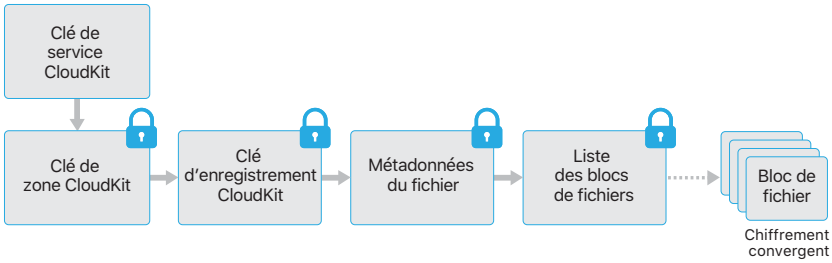
iCloud Drive ajoute des clés basées sur le compte pour protéger les documents enregistrés dans iCloud. À l'instar des autres services iCloud, il divise le contenu des fichiers en plusieurs blocs qu'il chiffre avant de stocker les blocs chiffrés par le biais de services tiers. Les clés de contenu de fichier 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 service de 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 de droits applicatifs (entitlements). CloudKit prend en charge les bases de données publiques et les bases de données privées. Les bases de données publiques sont utilisées par toutes les copies 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 le biais 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 auprès d'iCloud.



Chiffrement de bout en bout de CloudKit

Apple Pay Cash, les données de santé, les mots-clés de l'utilisateur, Siri Intelligence et « Dis Siri » utilisent le chiffrement de bout en bout de CloudKit avec une clé de service CloudKit protégée par synchronisation des trousseaux iCloud. Pour ces conteneurs CloudKit, la hiérarchie des clés est intégrée au trousseau iCloud et partage, par conséquent, les caractéristiques de sécurité du trousseau iCloud. Les clés sont uniquement disponibles sur les appareils de confiance de l'utilisateur et non sur ceux d'Apple ou sur des appareils tiers. Si l'accès aux données de trousseau d'iCloud est perdu (consultez la section « Sécurité des dépôts » plus loin dans ce document), les données de CloudKit sont réinitialisées et si des données sont disponibles sur l'appareil local de confiance, elles sont à nouveau téléchargées dans CloudKit.

L'option Messages sur iCloud utilise également le chiffrement de bout en bout CloudKit avec une clé de service CloudKit protégée par la synchronisation des trousseaux iCloud. Si l'utilisateur a activé la sauvegarde iCloud, la clé de service CloudKit utilisée pour le conteneur Messages sur iCloud est synchronisée avec iCloud pour permettre à l'utilisateur de récupérer ses messages même s'il n'a plus accès au trousseau iCloud et à ses appareils de confiance. Cette clé de service iCloud est remplacée chaque fois que 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 sur une source d'alimentation et connecté à Internet via 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.

Options de récupération

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

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

Données sauvegardées par iCloud :

- enregistrements relatifs aux morceaux, films, programmes télévisés, apps et livres achetés : la sauvegarde iCloud d'un utilisateur comprend des informations relatives au contenu acheté présent sur l'appareil iOS de l'utilisateur, mais pas au contenu acheté lui-même. Lorsque l'utilisateur restaure ses données à partir de Sauvegarde iCloud, son contenu acheté est automatiquement téléchargé depuis l'iTunes Store, Apple Books ou l'App Store. Certains types de contenu ne sont pas automatiquement téléchargés dans tous les pays ou régions, et les achats précédents peuvent être indisponibles s'ils ont été remboursés ou ne sont plus disponibles dans le store. L'historique complet des achats est associé à l'identifiant Apple d'un utilisateur ;
- photos et vidéos sur les appareils iOS d'un utilisateur : il convient de remarquer que si un utilisateur active la photothèque iCloud sur son appareil iOS 8.1 ou ultérieur ou Mac OS X 10.10.3 ou ultérieur, ses photos et vidéos sont déjà stockées dans iCloud de sorte qu'elles ne sont pas incluses dans la sauvegarde iCloud de l'utilisateur ;
- contacts, événements de calendrier, rappels et notes ;
- réglages d'appareil ;
- données d'app ;
- historique des appels et sonneries ;
- organisation de l'écran d'accueil et des apps ;
- configuration HomeKit ;
- code secret de messagerie visuelle (requiert la carte SIM utilisée lors de la sauvegarde) ;
- messages iMessage, Business Chat, SMS et MMS (requiert la carte SIM utilisée lors de la sauvegarde).

Remarque : lorsque l'option Messages sur iCloud est activée, les messages iMessage, Business Chat, SMS et MMS sont supprimés de la sauvegarde iCloud de l'utilisateur et stockés dans un conteneur CloudKit chiffré de bout en bout pour Messages. La sauvegarde iCloud de l'utilisateur conserve une clé pour ce conteneur. Si l'utilisateur désactive par la suite l'option Sauvegarde iCloud, la clé de ce conteneur est remplacée, la nouvelle clé est uniquement stockée dans le trousseau iCloud (dont l'accès est interdit à Apple et aux tiers) et les nouvelles données écrites dans le conteneur ne peuvent être déchiffrées à l'aide de l'ancienne clé de conteneur.

Si des fichiers sont créés dans des classes de protection de données (Data Protection) 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 sans protection (No Protection) sont chiffrés durant le transfert.

Le conteneur de clés de Sauvegarde iCloud contient des clés asymétriques (Curve25519) pour chaque classe Data Protection, 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, consultez la partie intitulée « Protection des données du trousseau » de la section « Chiffrement et protection des données » de ce document.

La sauvegarde est stockée dans le compte iCloud de l'utilisateur et est constituée d'une copie de ses fichiers, ainsi que 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, afin que toute modification du mot de passe iCloud n'ait 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 ensuite 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 (Data Protection).

Trousseau iCloud

Intégration de Safari et du trousseau iCloud
Safari peut générer automatiquement des chaînes de caractères aléatoires cryptographiquement complexes à utiliser comme mots de passe de site web, stocker ces mots de passe dans le trousseau et les synchroniser avec d'autres appareils. Les éléments de trousseau sont transférés d'un appareil à l'autre en passant par des serveurs Apple, mais ils sont chiffrés de telle manière que leur contenu ne peut être lu ni par des appareils Apple, ni par des appareils tiers.

Le trousseau iCloud donne aux utilisateurs la possibilité de synchroniser de manière sécurisée leurs mots de passe entre 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 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 (via 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 (salt 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 et il ne peut être modifié 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 signale que l'utilisateur a précédemment établi, dans iCloud, un cercle de synchronisation 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. Pour terminer, 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 à travers l'espace de stockage des valeurs de clé iCloud ou à les stocker le cas échéant dans CloudKit. 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 ensuite chiffré et ne peut être déchiffré que par un appareil faisant partie du cercle de confiance de l'utilisateur. Il ne peut être déchiffré ni 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 propres à chaque appareil, tels que les identités VPN, ne peuvent pas quitter leur appareil. Seuls les éléments possédant l'attribut `kSecAttrSynchronizable` sont synchronisés. Apple a défini cet attribut pour les données d'utilisateur 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 tierces 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 un service d'authentification secondaire et de dépôt sécurisé créé spécifiquement par Apple pour prendre cette fonctionnalité en charge. 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'identification à deux facteurs l'est également sur le compte de l'utilisateur, le code de verrouillage de l'appareil est utilisé pour récupérer un trousseau déposé. Si l'identification à deux facteurs n'a pas été configurée, l'utilisateur est invité à créer un code de verrouillage de sécurité iCloud en fournissant un code à six chiffres. Toutefois, en l'absence d'identification à deux facteurs, les utilisateurs peuvent définir leur propre code plus long ou laisser leur appareil créer automatiquement un code cryptographiquement aléatoire qu'il peut 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 du cluster de module de sécurité matériel (HSM) destiné à stocker l'enregistrement en dépôt. Ce dernier devient alors l'enregistrement en dépôt iCloud de l'utilisateur.

Si l'utilisateur a décidé d'accepter un code de sécurité cryptographiquement 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 fournit un second niveau d'authentification lors de la récupération d'un trousseau. L'utilisateur reçoit un SMS 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. Topographiquement placés derrière iCloud se trouvent les clusters HSM qui hébergent les fiches de dépôt. Chacun d'eux possède une clé utilisée pour chiffrer les enregistrements en dépôt placés sous sa garde comme évoqué précédemment dans ce document.

Pour récupérer un trousseau, les utilisateurs doivent s'authentifier avec leur nom d'utilisateur et leur mot de passe iCloud et répondre à un SMS envoyé à leur numéro de téléphone enregistré. Après avoir effectué cette opération, ils doivent également saisir leur code de sécurité iCloud. Le cluster HSM vérifie que l'utilisateur connaît son code de sécurité iCloud à l'aide du protocole Secure Remote Password (SRP), mais ce code n'est pas envoyé à Apple. Chaque membre du cluster vérifie indépendamment que l'utilisateur n'a pas dépassé le nombre maximum de tentatives autorisées de récupération de son enregistrement comme indiqué ci-dessous. Si cela est confirmé par une majorité de clusters, 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 maximum de tentatives d'authentification et de récupération d'un enregistrement en dépôt est fixé à 10. Après plusieurs tentatives manquées, l'enregistrement est verrouillé et l'utilisateur doit appeler l'assistance Apple pour pouvoir effectuer des tentatives supplémentaires. Après la 10e tentative manquée, le cluster 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 du cluster 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 le cluster HSM. Si cela devait se produire, le propriétaire de chaque trousseau protégé par le cluster reçoit un message lui annonçant la perte de leur enregistrement placé en dépôt. Ils peuvent alors décider de se réenregistrer auprès du service.

Siri

Les utilisateurs peuvent, en parlant naturellement, demander à Siri d'envoyer des messages, de programmer des rendez-vous, de passer 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 en veillant à n'utiliser qu'une quantité absolument minimale de données personnelles et à assurer une protection totale de ces données.

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 à la réactivation de Siri.

Pour mettre 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 morceaux, artistes et listes de lecture), les noms des listes de rappels, ainsi que les noms et les relations définies 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 10 minutes d'inactivité, quoi qu'il arrive.

Lorsqu'une requête Siri est formulée sur l'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, la requête fait également état de 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 depuis Contacts sont utilisés. La commande de l'action identifiée est ensuite renvoyée à l'appareil afin d'être exécutée.

De nombreuses fonctionnalités 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 de fiches, transcriptions et données associées sans identifiant sont susceptibles de continuer à être employées par Apple pour l'amélioration continue et le contrôle de qualité de Siri au-delà de deux ans. De plus, certains enregistrements faisant référence à la musique, aux équipes sportives et leurs joueurs, ainsi qu'au monde des affaires et divers points d'intérêt sont enregistrés de façon similaire 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 par Siri.

Les utilisateurs peuvent également invoquer Siri sur l'Apple Watch en levant leur montre jusqu'à proximité de leur bouche et en lançant une requête vocale Siri. Siri est activé de cette manière lorsque les deux conditions suivantes sont satisfaites :

- un modèle d'apprentissage machine sur l'appareil détecte le signal acoustique de la voix humaine à proximité de l'appareil ;
- un deuxième modèle d'apprentissage machine sur l'appareil identifie un profil de mouvement et une position d'appareil correspondant au geste Lever pour parler.

Lorsque cette combinaison de mouvement 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 par Siri.

Suggestions Siri

Les suggestions Siri relatives aux apps et aux raccourcis sont générées en faisant appel à l'apprentissage machine sur l'appareil. Aucune donnée n'est transmise à Apple à l'exception des informations anonymes relatives aux signaux susceptibles d'être de bons prédicteurs pour les raccourcis ou les lancements d'app.

Raccourcis dans Siri

Les raccourcis ajoutés à Siri sont synchronisés via iCloud sur tous les appareils Apple et chiffrés à l'aide du chiffrement CloudKit de bout en bout. Les expressions liées à des raccourcis sont synchronisées avec le serveur Siri pour la reconnaissance vocale et associées à l'identifiant aléatoire Siri décrit dans la section Siri. Apple ne reçoit pas le contenu des raccourcis qui sont stockés localement dans un dossier de données sécurisé.

App Raccourcis

Les raccourcis personnalisés de l'app Raccourcis sont synchronisés de manière facultative sur les appareils Apple via iCloud. Il est également possible de partager des raccourcis avec d'autres utilisateurs via iCloud.

Les raccourcis personnalisés sont polyvalents ; ils sont semblables à des scripts ou à des programmes. Un système de quarantaine est utilisé pour isoler les raccourcis téléchargés depuis Internet. L'utilisateur est averti la première fois qu'il essaye d'utiliser le raccourci et a la possibilité d'inspecter ce dernier et de consulter certaines informations concernant l'origine du raccourci.

Les raccourcis personnalisés peuvent également exécuter du code JavaScript spécifié par l'utilisateur sur des sites web dans Safari lorsqu'ils sont invoqués à partir de la feuille de partage. En guise de protection contre tout code JavaScript malveillant susceptible, par exemple, de tromper l'utilisateur en le poussant à exécuter un script sur un site web de médias sociaux qui recueille ses données, des mises à jour de définitions de logiciels malveillants sont téléchargées afin d'identifier les scripts malveillants au moment où ils sont exécutés. La première fois qu'un utilisateur exécute du code JavaScript sur un domaine, il est invité à autoriser l'exécution de raccourcis contenant du code JavaScript sur la page de ce domaine actuellement affichée.

Suggestions Safari, Suggestions Siri dans les recherches, Recherche, #images, app News et widget News dans les pays sans l'app News

Suggestions Safari, Suggestions Siri dans les recherches, Recherche, #images, l'app News et le widget News dans les pays sans l'app News affichent des suggestions dépassant le cadre de l'appareil des utilisateurs, provenant de sources telles que Wikipédia, l'iTunes Store, l'actualité locale, les résultats de cartes et l'App Store, mais aussi des suggestions avant même la saisie.

Lorsqu'un utilisateur commence à saisir dans la barre d'adresse de Safari, ouvre ou utilise des suggestions Siri dans les recherches, utilise Recherche, ouvre des #images, utilise la fonction Recherche dans l'app News ou utilise le widget News dans les pays sans l'app News, le contexte suivant est envoyé sous forme chiffrée par HTTPS à Apple pour offrir à l'utilisateur des résultats appropriés :

- un identifiant qui change toutes les 15 minutes pour préserver la confidentialité ;
- la requête de recherche de l'utilisateur ;
- l'exécution de requête la plus probable basée sur le contexte et les recherches passées localement mises en cache ;
- la localisation approximative de son appareil, si le Service de localisation pour les suggestions géodépendantes est activé. 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 Service de

localisation pour les Suggestions géodépendantes dans Réglages. Si Service de localisation est désactivé, Apple peut utiliser l'adresse IP de l'appareil pour déduire une position approximative ;

- le type d'appareil et si Suggestions Siri est utilisé dans la fonction de recherche, Safari, Recherche, l'app News ou Messages ;
- le type de connexion ;
- l'information relative aux trois dernières apps utilisées sur l'appareil (pour préciser davantage le contexte de la recherche) (seules les apps reprises dans une liste d'autorisations tenue à jour par Apple et contenant les apps populaires utilisées au cours des 3 dernières heures sont incluses) ;
- la liste des applications les plus utilisées sur l'appareil ;
- les préférences de langue, de pays et de saisie ;
- si l'appareil de l'utilisateur peut accéder à des services de musique ou vidéo avec abonnement, les données telles que le nom du service et le type d'abonnement peuvent être envoyées à Apple ; le nom, le numéro et le mot de passe du compte ne sont pas envoyés à Apple ;
- la représentation résumée et regroupée 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 améliorer la qualité des futurs résultats. Ces informations sont liées uniquement au même identifiant de session de 15 minutes et non à un utilisateur donné. Les commentaires incluent certaines des informations contextuelles décrites précédemment ainsi que les informations d'interaction telles que :

- les temps entre les interactions et les requêtes réseau des recherches ;
- 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 sélectionné s'il est local ;
- un indicateur précisant si l'utilisateur a sélectionné le résultat.

Apple conserve pendant 18 mois les historiques de Suggestions comprenant les requêtes, le contexte et les commentaires. Un sous-ensemble de journaux est conservé pendant un maximum de cinq ans. Il s'agit par exemple de requêtes, d'éléments linguistiques, de domaines, de lieux approximatifs et de mesures d'agrégation.

Dans certains cas, Suggestions peut transférer des requêtes relatives à des mots et des phrases courants à un partenaire agréé, afin de recevoir et d'afficher les résultats de recherche de ce partenaire. Apple intercepte les requêtes de manière que les partenaires ne reçoivent pas les adresses IP d'utilisateurs ni ne consultent les commentaires. La communication avec le partenaire est chiffrée via HTTPS. Pour les requêtes fréquentes, Apple fournit au partenaire un contexte de recherche comprenant la ville, le type d'appareil et la langue du client pour améliorer la pertinence des résultats de recherche.

Pour comprendre et améliorer la pertinence géographique des suggestions et les performances à travers différents types de réseaux, les informations suivantes sont consignées sans identifiant de session :

- l'adresse IP partielle (sans le dernier octet dans le cas des adresses IPv4 et sans les derniers 80 bits pour les adresses IPv6) ;
- le lieu approximatif ;
- l'heure approximative de la requête ;
- la latence/le taux de transfert ;
- la taille de la réponse ;
- le type de connexion ;
- la langue ;
- le type d'appareil et l'app formulant la requête.

Prévention intelligente du suivi dans Safari

La prévention intelligente du suivi (ou ITP, de l'anglais « Intelligent Tracking Prevention ») fait partie de la politique favorable au respect de la vie privée appliquée par défaut par Safari en ce qui concerne les cookies et les données des sites web. Elle permet d'interdire le suivi à travers les sites en limitant l'accès aux cookies et à d'autres données de sites web.

L'ITP recueille des statistiques sur les ressources chargées (images, scripts, etc.) ainsi que sur les interactions de l'utilisateur telles que les éléments touchés à l'écran et le texte saisi au clavier. Un modèle d'apprentissage machine est utilisé pour le classement, sur l'appareil, des noms de domaine capables de suivre l'utilisateur à travers plusieurs sites, en se basant sur les statistiques recueillies.

Lorsqu'un domaine est classé parmi les domaines disposant de capacités de suivi, l'ITP partitionne immédiatement ses cookies si l'utilisateur a précédemment interagi avec ce domaine en tant que première partie ; s'il s'agit de domaines classés avec lesquels l'utilisateur n'a pas interagi, l'ITP commence immédiatement à bloquer ses cookies. Exemple :

- Le site vidéo.exemple propose à ses abonnés un service sans publicité et dispose de nombreuses vidéos incorporées dans d'autres sites web.
- Un utilisateur ouvre une session sur vidéo.exemple, puis sur d'autres sites web proposant du contenu vidéo.exemple incorporé.
- L'ITP classe vidéo.exemple parmi les sites disposant de capacités de suivi et, par conséquent, partitionne ses cookies.
- Lorsqu'un utilisateur visite le site journal.exemple qui propose du contenu incorporé provenant de vidéo.exemple, les cookies fournis à vidéo.exemple sont des cookies partitionnés propres à vidéo.exemple sur journal.exemple.

Tout contenu tiers incorporé peut demander à un utilisateur l'accès à ses cookies de première partie via l'API d'accès au stockage. Lorsqu'un utilisateur touche ou clique sur du contenu tiers incorporé faisant appel à l'API d'accès au stockage, Safari affiche une invite demandant si l'utilisateur souhaite autoriser la tierce partie à accéder à ses cookies et données de sites web, ce qui permet à la tierce partie de le suivre sur le domaine de première partie. Si l'utilisateur sélectionne Autoriser, le contenu tiers incorporé est autorisé à accéder à ses cookies de première partie pendant la durée de consultation de cette page ; lors des visites ultérieures, le contenu tiers incorporé aura accès à ses cookies de

première partie une fois que l'utilisateur aura interagi avec le contenu incorporé et que ce dernier aura fait appel à l'API d'accès au stockage. Et comme l'utilisateur aura précédemment autorisé cet accès, aucune nouvelle invite ne sera affichée. La décision de l'utilisateur est maintenue pour la combinaison première partie et tierce partie et est effacée lorsque l'utilisateur efface son historique Safari.

Les cookies existants provenant de domaines classés comme disposant de capacités de suivi sont supprimés si l'utilisateur n'a plus interagi avec le domaine concerné – directement ou par l'intermédiaire de l'API d'accès au stockage – depuis 30 jours d'utilisation active de Safari. Après 30 jours sans interaction, un domaine classé comme disposant de capacités de suivi ne peut en outre pas activer de nouveaux cookies. Safari n'autorise jamais l'accès aux autres données de sites web de première partie dans des contextes tiers.

L'isolation des données de première partie et de tierce partie effectuée par l'ITP contribue à interdire l'utilisation de cookies et de données de sites web à des fins de suivi à travers plusieurs sites. Apple n'a pas accès aux noms des domaines dont les statistiques ont été recueillies par un appareil particulier ou qui ont été classés comme disposant de capacités de suivi.

Outre le blocage des cookies tiers provenant de domaines classés comme disposant de capacités de suivi, l'ITP limite à la seule origine de la page les informations de référant HTTP envoyées à de tels domaines tiers.

Gestion des mots de passe d'utilisateur

iOS propose aux utilisateurs plusieurs fonctions leur permettant de s'authentifier en toute simplicité de manière sûre et pratique auprès d'apps et de sites web tiers faisant appel à des mots de passe pour l'authentification. Les mots de passe sont enregistrés dans un trousseau spécial intitulé Remplissage automatique des mots de passe, contrôlé par l'utilisateur et gérable à partir de Réglages > Mots de passe et comptes > Mots de passe Web/apps. Les apps ne peuvent pas accéder à ce trousseau sans l'autorisation de l'utilisateur. Les informations d'identification enregistrées dans le trousseau Remplissage automatique des mots de passe sont synchronisées à travers les appareils avec le trousseau iCloud quand ce dernier est activé.

Le gestionnaire de mots de passe du trousseau iCloud et Remplissage automatique des mots de passe fournissent les fonctions suivantes :

- remplissage des champs d'identification dans les apps et sur les sites web ;
- génération de mots de passe complexes ;
- enregistrement des mots de passe d'app et de site web dans Safari ;
- partage sécurisé des mots de passe avec les contacts de l'utilisateur ;
- transmission de mots de passe à une Apple TV proche 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 le trousseau Remplissage automatique des mots de passe en utilisant les deux API suivantes :

`SecRequestSharedWebCredential`

`SecAddSharedWebCredential`

L'accès n'est accordé à une app iOS que si le développeur de l'app et l'administrateur du site web donnent tous deux leur approbation, et si l'utilisateur a donné 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. Le droit contient la liste des noms de domaine complets des sites web associés, et les sites web doivent placer sur leur serveur un fichier répertoriant les identifiants d'app uniques des apps approuvées par Apple.

Lorsqu'une app incluant le droit com.apple.developer.associated-domains est installée, iOS envoie une requête TLS à chaque site web répertorié pour demander l'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 destinés aux apps

iOS permet aux utilisateurs de saisir des noms d'utilisateur et des mots de passe dans les champs prévus à cet effet dans des apps, en touchant une capacité de suggestion de « clé » de la barre QuickType du clavier iOS. Le système exploite le même mécanisme d'association app-website basé sur le fichier apple-app-site-association pour associer étroitement des apps et des sites web. Cette interface ne communique aucune information d'identification à l'app tant que l'utilisateur n'a pas consenti à communiquer une telle information à l'app en question. Quand iOS établit qu'un site web et une app entretiennent une relation de confiance, la barre QuickType suggère alors directement des informations d'identification à saisir dans l'app. Cela permet aux utilisateurs de divulguer des informations d'identification enregistrées sur Safari à des apps ayant des propriétés de sécurité identiques, mais sans forcer ces apps à adopter une API.

Lorsqu'une app et un site web entretiennent une relation de confiance et qu'un utilisateur soumet des informations d'identification au sein d'une app, iOS peut inviter l'utilisateur à enregistrer ces informations dans le trousseau Remplissage automatique des mots de passe en vue d'une utilisation ultérieure.

Mots de passe complexes automatiques

Lorsque le trousseau iCloud est activé, iOS crée des mots de passe aléatoires complexes et uniques lorsqu'un utilisateur enregistre un mot de passe ou modifie son mot de passe existant dans une app ou sur un site web dans Safari. Les utilisateurs doivent choisir de ne pas utiliser de mots de passe complexes. Les mots de passe générés sont enregistrés dans le trousseau et synchronisés à travers les appareils avec le trousseau iCloud si ce dernier est activé.

Les mots de passe générés par iOS ont une longueur par défaut de 20 caractères. Ils contiennent un chiffre, un caractère majuscule, deux tirets et 16 caractères minuscules. Ces mots de passe générés sont complexes et contiennent 71 bits d'entropie.

iOS génère des mots de passe dans les apps et dans Safari en se basant sur une heuristique qui détermine qu'un champ de saisie est destiné à la création de mots de passe. Si l'heuristique ne parvient pas à reconnaître un contexte de mot de passe destiné à la création de mots de passe, les développeurs d'app peuvent définir UITextContentType.newPassword sur leur champ de texte et les développeurs de sites web peuvent définir autocomplete="new-password" sur leurs éléments <input>.

Les apps et les sites web peuvent fournir à iOS des règles permettant de s'assurer que les mots de passe générés sont compatibles avec le service concerné. iOS peut alors générer les mots de passe les plus complexes possible conformément à ces règles. Les développeurs fournissent ces règles en utilisant UITextInputPasswordRules ou l'attribut passwordrules sur leurs éléments <input>.

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

AirDrop

Si iCloud est activé, les utilisateurs peuvent transmettre à un autre appareil, via AirDrop, des informations d'identification enregistrées incluant les noms des sites web destinataires, leur nom d'utilisateur et leur mot de passe. L'envoi d'informations d'identification avec AirDrop fonctionne toujours en mode Contacts uniquement, quels que soient les réglages adoptés par l'utilisateur. (Reportez-vous à « Sécurité AirDrop » pour en savoir plus.) Sur l'appareil destinataire, après le consentement de l'utilisateur, les informations d'identification sont enregistrées dans le trousseau Remplissage automatique des mots de passe de l'utilisateur.

Apple TV

Remplissage automatique des mots de passe est disponible pour remplir les champs d'informations d'identification dans des apps sur l'Apple TV. Lorsque l'utilisateur se concentre sur un champ de nom d'utilisateur ou de mot de passe sous tvOS, l'Apple TV lance une demande de remplissage automatique des mots de passe via Bluetooth Low Energy (BLE).

Tout iPhone situé à proximité affiche un message invitant l'utilisateur à partager des informations d'identification avec l'Apple TV. Les communications entre un iPhone et une Apple TV utilisant le même compte iCloud sont chiffrées durant ce processus. Si l'iPhone est connecté à un compte iCloud différent de celui de l'Apple TV :

- un code PIN est utilisé pour établir une connexion chiffrée ;
- l'iPhone doit être déverrouillé et se trouver à proximité de la télécommande Siri Remote associée à cette Apple TV pour recevoir cette invite.

Une fois la connexion chiffrée établie en utilisant le chiffrement de la liaison Bluetooth LE, les informations d'identification sont envoyées à l'Apple TV et automatiquement insérées dans les champs de texte correspondants de l'app.

Extensions de fournisseur d'informations d'identification

Les utilisateurs peuvent désigner une application tierce compatible comme fournisseur d'informations d'identification pour le Remplissage automatique dans les réglages Mots de passe et comptes. Ce mécanisme est basé sur des extensions. L'extension du fournisseur d'informations d'identification doit fournir une fenêtre de sélection d'informations d'identification et peut, de manière facultative, fournir des métadonnées iOS liées aux informations d'identification enregistrées afin qu'elles soient proposées directement dans la barre QuickType. Les métadonnées comprennent le site web des informations d'identification et le nom d'utilisateur associé, mais pas le mot de passe. iOS communique ensuite avec l'extension pour obtenir le mot de passe lorsque l'utilisateur choisit de l'introduire dans une app ou un site web dans Safari. Les métadonnées d'informations d'identification sont stockées dans l'environnement sandbox du fournisseur d'informations d'identification et sont automatiquement supprimées lorsqu'une app est désinstallée.

Contrôle des appareils

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 (BYOD), par exemple.

Les organisations peuvent utiliser des moyens comme la protection par code de verrouillage, les profils de configuration, l'effacement à distance ou des solutions de gestion d'appareils mobiles (MDM) tierces pour gérer leurs parcs d'appareils et garantir la sécurité de leurs données, même si leurs employés y accèdent par le biais de leurs propres appareils iOS.

Protection par code de verrouillage

L'utilisateur peut choisir par défaut un code PIN constitué de chiffres. Sur les appareils dotés de Touch ID ou Face ID, la longueur minimale du code de verrouillage est de quatre chiffres. Les utilisateurs peuvent indiquer un code de verrouillage alphanumérique plus long en sélectionnant Code alphanumérique personnalisé dans les Options de code de Réglages > Code. Les codes de verrouillage plus complexes et plus longs sont plus difficiles à deviner ou à attaquer et sont recommandés.

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

- autoriser des valeurs simples ;
- exiger des valeurs alphanumériques ;
- imposer une longueur minimale de code de verrouillage ;
- imposer un nombre minimal de caractères complexes ;
- imposer une durée limite de validité du code de verrouillage ;
- conserver un degré d'historique des codes de verrouillage ;
- appliquer un délai de blocage automatique ;
- offrir une période de grâce pour le blocage de l'appareil ;
- limiter le nombre de tentatives manquées ;
- autoriser Touch ID ou Face ID.

Pour en savoir plus sur chaque règlement administrateur, consultez : https://help.apple.com/deployment/mdm/#/mdm4D6A472A

Pour en savoir plus sur chaque règlement de développement, consultez : https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/

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, telle que la synchronisation de données.

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

De plus, sous iOS 10 ou ultérieur, certains services, notamment la synchronisation de photos, nécessitent que l'appareil soit déverrouillé pour commencer.

Dans iOS 11 ou ultérieur, les services ne démarrent que si l'appareil vient d'être déverrouillé.

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 ultérieur, l'utilisateur est également tenu de saisir son code de verrouillage. Une fois que l'utilisateur a accepté cette demande, l'hôte et l'appareil échangent et enregistrent des clés publiques RSA 2048 bits. L'hôte reçoit ensuite une clé 256 bits capable de débloquer un conteneur de clés en dépôt sur l'appareil (reportez-vous à la partie consacrée au « Conteneur de clés de dépôt » dans la section « Conteneurs de clés » de ce 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, celle-ci expire. Ce délai est réduit à 30 jours pour iOS 11 ou ultérieur.

Pour en savoir plus, consultez la page suivante :
https://support.apple.com/HT6331

Certains services, comme com.apple.pcapd, ne peuvent fonctionner que via USB. De même, le service com.apple.file_relay requiert un profil de configuration signé par Apple pour être installé.

Sous iOS 11 ou ultérieur, l'Apple TV peut utiliser le protocole Secure Remote Password pour effectuer 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 en savoir plus, consultez la page suivante :
https://support.apple.com/HT5868

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 données. Un profil de configuration destiné à fournir une configuration d'e-mail, par exemple, peut également spécifier une politique de code de verrouillage pour un appareil. Les utilisateurs ne peuvent accéder à leurs e-mails que si leur code de verrouillage est conforme aux exigences de l'administrateur.

Les profils de configuration iOS contiennent plusieurs réglages qu'il est possible de spécifier :

- règlements inhérents aux codes de verrouillage ;
- les restrictions liées aux fonctionnalités de l'appareil (comme la désactivation de la caméra) ;
- les réglages Wi-Fi ;
- les réglages VPN ;
- les réglages de serveur de messagerie ;
- les réglages Exchange ;
- les réglages de service d'annuaire LDAP ;
- les réglages de service de calendrier CalDAV ;
- les clips web ;
- les informations d'identification et les clés ;
- les réglages avancés de réseau mobile.

Pour afficher la liste à jour à l'attention des administrateurs, consultez : https://help.apple.com/deployment/mdm/#/mdm5370d089

Pour afficher la liste à jour à l'attention des développeurs, consultez : https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/

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 en utilisant 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 de verrouillage. Dans la mesure où de nombreux utilisateurs possèdent leurs propres appareils iOS, les profils de configuration qui lient un appareil à une solution MDM peuvent être éliminés, mais une telle action supprime également toutes les informations, données et apps 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 e-mail ou les recevoir via une connexion sans fil à partir d'une solution MDM. Lorsqu'un utilisateur configure un appareil dans Apple School Manager ou Apple Business Manager, l'appareil télécharge et installe un profil pour l'enregistrement MDM.

Mobile Device Management - Gestion des appareils mobiles (MDM)

La prise en charge de MDM par iOS permet aux entreprises de configurer et de gérer en toute sécurité des déploiements d'iPhone, d'iPad, d'Apple TV et de Mac au sein de leur structure. Les fonctionnalités MDM s'appuient sur des technologies iOS existantes telles que les profils de configuration, l'enregistrement en mode OTA et le service Apple Push Notification. Par exemple, le service APN sert à réactiver l'appareil afin qu'il puisse communiquer directement avec sa solution MDM à travers une connexion sécurisée. Aucune information confidentielle ou propriétaire n'est transmise par le service APN.

Grâce à la gestion MDM, les services IT peuvent enregistrer des appareils iOS dans des environnements d'entreprise, configurer et mettre des réglages à jour à travers une connexion sans fil, contrôler la conformité aux règles de la société, gérer des règles de mise à jour de logiciels et même, verrouiller ou supprimer à distance le contenu des appareils gérés.

Pour en savoir plus sur MDM, consultez :

- https://www.apple.com/fr/iphone/business/it/management.html
- https://help.apple.com/deployment/ios/#/ior07301dd60
- https://help.apple.com/deployment/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 de partager un iPad sans partager de documents et de données. Chaque étudiant se voit attribuer son propre répertoire de départ qui est créé sous forme de volume APFS protégé par les informations d'identification de l'utilisateur. iPad partagé nécessite l'usage 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, configuré pour un usage par plusieurs élèves. Les données des élèves sont partitionnées en répertoires de départ distincts, chacun dans son propre domaine de protection de données et protégé par des autorisations UNIX et par un environnement contrôlé de type sandboxing.

Connexion à un iPad partagé

Lorsqu'un élève ouvre une session, l'identifiant Apple géré est authentifié par le biais des serveurs d'identité d'Apple en faisant appel au protocole SRP. Si l'ouverture de session aboutit, un jeton d'accès court terme, spécifique à l'appareil, est accordé. Si l'étudiant a utilisé l'appareil auparavant, il dispose déjà d'un compte local qu'il peut déverrouiller à l'aide des mêmes informations d'identification.

Si l'étudiant n'a pas utilisé l'appareil auparavant, un nouvel identifiant d'utilisateur UNIX, un volume APFS avec le répertoire de départ de l'utilisateur et un trousseau logique lui sont fournis. Si l'appareil n'est pas connecté à Internet (par exemple, si l'étudiant est en voyage de classe), l'identification peut se produire en dépit du compte local pendant un nombre de jours limité. Dans ce cas, seuls les utilisateurs disposant de comptes locaux préexistants peuvent se connecter. Une fois le délai expiré, les étudiants sont tenus de s'authentifier en ligne, même s'ils disposent déjà d'un compte local.

Après le déverrouillage ou la création du compte local de l'étudiant, si ce dernier s'authentifie à distance, le jeton court terme délivré par les serveurs d'Apple est converti en jeton iCloud permettant d'ouvrir une session sur iCloud. Les réglages de l'étudiant sont ensuite restaurés, et ses documents et données sont synchronisés depuis 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 au fur et à mesure de leur création ou de leur modification. En outre, un mécanisme de synchronisation en arrière-plan s'assure que les modifications sont envoyées à iCloud une fois que l'élève a fermé sa session. Après la synchronisation en arrière-plan de cet utilisateur, son volume APFS est démonté et ne peut plus être monté à nouveau sans que l'utilisateur indique ses informations d'identification.

Déconnexion d'un iPad partagé

Lorsqu'un élève se déconnecte d'un iPad partagé, le conteneur de clés d'utilisateur de cet élève est immédiatement verrouillé et toutes les apps sont fermées. Pour accélérer la procédure lorsqu'un nouvel élève se connecte, le système reporte temporairement certaines actions de connexion ordinaires et présente une fenêtre de connexion au nouvel élève. Si un élève se connecte durant cette période (d'environ 30 secondes), l'iPad partagé effectue le nettoyage reporté dans le cadre de la procédure de connexion au compte du nouvel étudiant. Toutefois, si l'iPad partagé demeure inactif, cela déclenche le nettoyage reporté. Durant la phase de nettoyage, la fenêtre de connexion est redémarrée comme si une autre déconnexion s'était produite.

Mise à niveau d'un iPad partagé

Lorsqu'un iPad partagé est mis à niveau depuis une version antérieure à iOS 10.3 vers une version 10.3 ou ultérieure, une conversion de système de fichiers se produit une seule fois pour convertir la partition de données HFS+ en volume APFS. Si un répertoire de départ d'un utilisateur est alors présent sur le système, ce répertoire demeure sur le volume de données principal au lieu d'être converti vers des volumes APFS individuels.

Lorsque des étudiants supplémentaires se connectent, leurs répertoires de départ sont également placés sur le volume de données principal. De nouveaux comptes d'utilisateur ne sont pas créés avec leur volume APFS, comme décrit précédemment, tant que les comptes d'utilisateur du volume de données principal n'ont pas tous été supprimés. De cette manière, pour s'assurer que les utilisateurs jouissent des protections et quotas supplémentaires attribués par APFS, soit l'iPad doit être mis à niveau vers la version 10.3 ou ultérieure par le biais d'une procédure d'effacement et de réinstallation, soit tous les comptes d'utilisateur de l'appareil doivent être supprimés à l'aide de la commande MDM « Supprimer l'utilisateur ».

Pour en savoir plus sur les iPad partagés, consultez :
https://help.apple.com/deployment/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'enregistrement automatique d'appareils dans des solutions MDM, 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 enseignants.

Pour en savoir plus sur Apple School Manager, consultez la page : https://help.apple.com/schoolmanager/

Apple Business Manager

Apple Business Manager est un portail web simple destiné aux administrateurs informatiques qui souhaitent déployer des appareils iOS, macOS et tvOS à partir d'un poste unique. Utilisé conjointement avec votre solution de gestion d'appareils mobiles (MDM), il vous permet de configurer les réglages des appareils et d'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, consultez la page : https://help.apple.com/businessmanager/

Enregistrement d'appareils

Apple School Manager et Apple Business Manager fournissent un moyen rapide et rationnel de déployer des appareils iOS achetés par une organisation soit directement auprès d'Apple, soit à travers des opérateurs et des revendeurs agréés Apple participant au programme. Il est également possible d'utiliser Apple Configurator 2 pour ajouter à Apple School Manager et Apple Business Manager des appareils exécutant iOS 11 et tvOS 10.2 ou des versions ultérieures de ces systèmes après leur achat.

Les organisations peuvent ainsi enregistrer automatiquement ces appareils dans leur système de gestion MDM sans avoir à les manipuler physiquement ou à les préparer avant de les remettre à leurs utilisateurs. Après l'enregistrement dans l'un de ces programmes, les administrateurs se connectent au site web du programme et associent le programme à leur solution MDM. Les appareils achetés peuvent ensuite être attribués à leurs utilisateurs via MDM. Au cours de la configuration de l'appareil, la sécurité des données sensibles peut être améliorée en assurant les mesures de sécurité en place les mieux adaptées. Exemple :

- Obligez les utilisateurs à s'identifier dans le cadre de la procédure de configuration de départ lors de l'activation d'Assistant réglages sur l'appareil Apple.
- Fournissez une configuration préliminaire avec un accès limité et faites appel à une configuration d'appareil supplémentaire pour accéder aux données sensibles.

Une fois qu'un utilisateur a reçu son appareil, toutes les configurations, les restrictions ou les commandes MDM spécifiées sont automatiquement installées. Toutes les communications entre les appareils et les serveurs d'Apple sont chiffrées au cours du transfert par HTTPS (SSL).

Il est possible de simplifier davantage le processus de configuration en supprimant certaines étapes spécifiques dans l'Assistant réglages pour iOS, tvOS et macOS, afin que les utilisateurs puissent être rapidement opérationnels. Les administrateurs ont également la possibilité de contrôler si les utilisateurs peuvent supprimer le profil MDM de leur appareil et de s'assurer que les restrictions sur ces appareils sont en place dès le départ. L'appareil, une fois déballé et activé, peut s'enregistrer dans la solution MDM de l'organisation et tous les livres, applications et réglages de gestion sont installés.

Apple Configurator 2

Outre le système de gestion MDM, Apple Configurator 2 pour macOS simplifie la configuration et la préconfiguration d'appareils iOS et d'Apple TV avant leur remise aux utilisateurs. Avec Apple Configurator 2, les appareils peuvent être rapidement préconfigurés avec des apps, des données, des restrictions et des réglages.

Apple Configurator 2 vous permet d'utiliser Apple School Manager ou Apple Business Manager pour enregistrer des appareils dans une solution MDM sans forcer les utilisateurs à faire appel à l'Assistant réglages. Apple Configurator 2 peut également être utilisé pour ajouter des appareils iOS et Apple TV à Apple School Manager ou Apple Business Manager après leur achat.

Pour en savoir plus sur Apple Configurator 2, consultez la page : https://help.apple.com/configurator/mac/

Supervision

Pendant la configuration d'un appareil, une entreprise peut le configurer pour qu'il soit supervisé. La supervision indique que l'appareil détenu appartient à l'entreprise et donne à cette dernière un contrôle supplémentaire sur sa configuration et ses restrictions. Avec Apple School Manager ou Apple Business Manager, la supervision peut être activée soit sans fil sur l'appareil dans le cadre de la procédure d'enregistrement MDM, soit manuellement à l'aide d'Apple Configurator 2. La supervision d'un appareil requiert l'effacement de ce dernier et la réinstallation du système d'exploitation.

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

Restrictions

Des restrictions peuvent être activées ou dans certains cas, désactivées, par les administrateurs pour empêcher les utilisateurs d'accéder à une app, un service ou une fonction spécifique de l'appareil. Les restrictions sont envoyées dans une entité qui est jointe à un profil de configuration. Les restrictions peuvent être appliquées aux appareils iOS, tvOS et macOS. Certaines restrictions d'un iPhone géré peuvent être reproduites sur un Apple Watch jumelé.

Pour afficher la liste des responsables informatiques, consultez : https://help.apple.com/deployment/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 de l'Effaceable Storage (Effaceable Storage), ce qui rend toutes les données illisibles. Une commande d'effacement à distance peut être envoyée via MDM, Exchange ou iCloud.

Lorsqu'une commande d'effacement à distance est déclenchée via MDM ou iCloud, l'appareil envoie une confirmation et effectue l'effacement des données. Pour l'effacement à distance via 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 cela a été 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 de verrouillage.

Mode Perdu

Si un appareil vient à être perdu ou volé, un administrateur MDM peut activer à distance le mode Perdu sur un appareil supervisé doté d'iOS 9.3 ou ultérieur. 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 vient à être 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 au travers d'un message sur l'écran de verrouillage ou d'une alerte dans l'écran d'accueil.

Verrouillage d'activation

Lorsque la fonctionnalité Localiser mon iPhone est activée, il est impossible de réactiver un appareil sans saisir les informations d'identification de l'identifiant Apple du propriétaire ou le code de verrouillage précédent de l'appareil.

Pour les appareils détenus par une organisation, il peut s'avérer judicieux de les superviser de sorte que la fonction 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 MDM compatible peut ensuite conserver un code de contournement lorsque le verrouillage d'activation est activé, ou peut utiliser ce code ultérieurement pour effacer 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. Une solution MDM 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 MDM 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 MDM 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 dans l'enseignement avec un identifiant Apple géré créé via Apple School Manager, la fonction Verrouillage d'activation peut être liée à l'identifiant Apple d'un administrateur plutôt qu'à celui de l'utilisateur ou être désactivée à l'aide du code de contournement de l'appareil.

Temps d'écran

Temps d'écran est une fonction iOS 12 qui permet à un utilisateur de comprendre et de contrôler le temps qu'il passe à utiliser des apps et Internet ou le temps que ses enfants consacrent à ces activités. Les utilisateurs peuvent ainsi :

- afficher leurs données d'utilisation ;
- fixer des limites d'utilisation d'app ou d'Internet ;
- configurer des temps d'arrêt ;
- appliquer des restrictions supplémentaires.

Pour un utilisateur qui gère sa propre utilisation d'appareil, les commandes et les données d'utilisation Temps d'écran peuvent être synchronisées à travers les appareils associés au même compte iCloud en appliquant le chiffrement CloudKit de bout en bout. Cela requiert l'activation de l'identification à deux facteurs sur le compte de l'utilisateur (la synchronisation est désactivée par défaut). Temps d'écran remplace la fonction Restrictions présente dans les anciennes versions d'iOS.

Lorsqu'un utilisateur efface son historique Safari ou supprime une app, les données d'utilisation correspondantes sont supprimées de l'appareil et de tous les appareils synchronisés.

Parents et Temps d'écran

Les parents peuvent également utiliser Temps d'écran sur des appareils iOS pour comprendre et contrôler la manière dont leurs enfants utilisent leurs appareils. Si le parent est un organisateur (dans les réglages Partage familial d'iCloud), il peut consulter les données d'utilisation et gérer les réglages Temps d'écran pour ses enfants. Les enfants sont prévenus lorsque leurs parents activent Temps d'écran et peuvent ainsi surveiller eux aussi leur propre utilisation. Lorsque des parents activent Temps d'écran pour leurs enfants, ils définissent un code de verrouillage afin que leurs enfants ne puissent effectuer des modifications. Les enfants auront la possibilité de désactiver cette surveillance le jour de leur 18e anniversaire (en fonction de leur pays de résidence).

Les données d'utilisation et les réglages de configuration sont transférés entre les appareils des parents et des enfants par le biais d'une connexion chiffrée de bout en bout au service d'identité Apple (IDS). Il se peut que ces données chiffrées soient brièvement stockées sur des serveurs IDS jusqu'à ce qu'elles soient lues par l'appareil destinataire (par exemple, dès que l'iPhone ou l'iPad est allumé s'il était éteint). Ces données ne peuvent pas être lues par Apple.

Analyse Temps d’écran

Si l’utilisateur active l’option « Partager l’analyse (iPhone+Watch) », seules les données anonymes suivantes sont collectées pour permettre à Apple de mieux comprendre la manière dont la fonction Temps d’écran est utilisée :

- La fonction Temps d’écran a-t-elle été activée durant l’Assistant réglages ou plus tard dans Réglages ?
- La fonction Temps d’écran est-elle activée ?
- La fonction Temps d’arrêt est-elle activée ?
- Combien de requêtes « Demander plus » ont-elles été effectuées ?
- Nombre de limites d’app

Apple ne collecte aucune donnée spécifique relative à l’utilisation des apps ou d’Internet. Les icônes d’app affichées dans la liste d’apps que l’utilisateur voit dans les informations d’utilisation Temps d’écran proviennent directement de l’App Store qui ne conserve aucune trace de ces requêtes.

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 mobile pour déterminer la position approximative de l'utilisateur. 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. Cela inclut la possibilité de désactiver l'inclusion des données de localisation dans les informations recueillies par les services d'analyse employés par Apple pour améliorer le système iOS, les informations de Siri basées sur la localisation, le contexte basé sur la localisation des recherches de Suggestions Siri, les conditions de circulation locales et les lieux significatifs visités dans le passé.

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
- Mouvements et activités physiques
- Services de géolocalisation
- Apple Music
- Votre activité musicale et vidéo
- 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 dans Réglages. iOS fournit également des restrictions qui interdisent tout mouvement de données entre les apps et les comptes installés par une solution MDM et ceux installés par l'utilisateur.

Politique de confidentialité

Pour lire la politique de confidentialité d'Apple, consultez : https://www.apple.com/fr/legal/privacy

Certificats et programmes de sécurité

Remarque : pour obtenir les dernières informations sur les certifications de sécurité, les procédures de validation et les instructions relatives à iOS, consultez : https://support.apple.com/HT202739

Certifications ISO 27001 et 27018

Apple a obtenu les certifications ISO 27001 et ISO 27018 pour le système de gestion de sécurité des informations pour l'infrastructure, le développement et les opérations prenant en charge ces produits et services : Apple School Manager, iTunes U, iCloud, iMessage, FaceTime, les identifiants Apple gérés, Siri et Pour l'école, conformément à la version 2.1 de la déclaration d'applicabilité (Statement of Applicability v2.1) en date du 11 juillet 2017. La conformité d'Apple aux normes ISO a été certifiée par la British Standards Institution. Le site web de BSI dispose de certificats de conformité pour les normes ISO 27001 et ISO 27018. Pour afficher ces certificats, rendez-vous sur :

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

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

Validation cryptographique (FIPS 140-2)

La conformité des modules cryptographiques 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 avec chaque version majeure, Apple transmet les modules à CMVP pour être revalidés lors de la publication du système d'exploitation iOS. Ce programme confirme l'intégrité des opérations cryptographiques pour les apps Apple et les apps tierces qui exploitent correctement les services cryptographiques d'iOS et les algorithmes approuvés.

Apple a reçu la validation FIPS 140-2 pour le module matériel incorporé intitulé **Apple Secure Enclave Processor (SEP) Secure Key Store (SKS) Cryptographic Module**, ce qui permet une utilisation approuvée des clés générées et gérées par SEP. Apple s'efforcera, si nécessaire, d'atteindre des niveaux de plus en plus élevés pour le module matériel à chaque publication de version majeure d'iOS.

Certification des critères communs (ISO 15408)

Depuis la parution d'iOS 9, Apple a obtenu des certifications iOS pour chaque version majeure d'iOS dans le cadre du programme Certification des critères communs et a étendu la couverture de ce programme afin d'inclure les éléments suivants :

- Profil de Protection (PP) des fondamentaux des appareils mobiles
  - Paquet étendu des agents de gestion des appareils mobiles
  - Paquet étendu des clients de réseau local sans fil
  - Module PP pour client VPN
- Profil de protection pour logiciel d'application
  - Paquet étendu des navigateurs Web

iOS 12 devrait inclure des certifications supplémentaires pour les éléments ci-dessous :

- Paquet étendu des clients de messagerie

Apple envisage d'étendre cette couverture à chaque version majeure d'iOS.

Apple joue un rôle actif au sein de la communauté technique internationale (ITC) dans le développement de profils de protection collaborative (cPP) actuellement indisponibles se concentrant sur l'évaluation des technologies de sécurité mobile des clés. Apple continue d'évaluer et de poursuivre les certifications visant les nouvelles versions et les mises à jour des profils cPP disponibles à ce jour et en cours de développement.

Solutions commerciales pour composants classifiés (CSfC)

Le cas échéant, Apple a également soumis la plateforme iOS et différents services à leur ajout 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 pour leur ajout dans la liste des composants du programme CSfC.

Pour consultez la liste des composants les plus récemment répertoriés, reportez-vous à l'adresse :
https://www.nsa.gov/resources/everyone/csfc/components-list/

Guides de configuration de sécurité

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

Récompense de sécurité Apple

Apple récompense les chercheurs qui font part à Apple des problèmes critiques qu'ils rencontrent. Afin d'avoir droit à la récompense de sécurité Apple, les chercheurs doivent fournir un rapport clair et des preuves concrètes du concept. La vulnérabilité doit affecter la dernière livraison d'iOS et s'avérer applicable au dernier matériel. Le montant exact du paiement est déterminé après examen par Apple. Les critères utilisés comprennent la nouveauté, la probabilité d'exposition et le degré d'interaction de l'utilisateur requis.

Une fois correctement partagés, Apple se donne pour priorité de résoudre les problèmes confirmés le plus rapidement possible. Selon les cas, Apple en fait état publiquement, sauf demande contraire.

Catégorie	Paiement maximal (en USD)
Composants du programme interne de démarrage sécurisé	200 000 $
Extraction d'éléments confidentiels protégés par le Secure Enclave	100 000 $
Exécution de code arbitraire avec privilèges de noyau	50 000 $
Accès interdit aux données de compte iCloud sur les serveurs d'Apple	50 000 $
Accès depuis un processus contrôlé aux données de l'utilisateur en dehors de l'environnement « sandbox »	25 000 $

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 de client-à-client. Pour les apps tierces, la combinaison de la signature obligatoire du code, du sandboxing et des autorisations fournit aux utilisateurs une protection inégalée dans l'industrie 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 des problèmes à Apple et l'abonnement aux notifications de sécurité, consultez la page : https://www.apple.com/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 d'amorçage logiciel	Bits dédiés du moteur AES Secure Enclave qui sont ajoutés à l'UID lors de la génération de clés à partir de l'UID. À chaque bit d'amorçage logiciel correspond un bit de verrouillage. Le système d'exploitation et la ROM de démarrage Secure Enclave peuvent modifier indépendamment la valeur de chaque bit d'amorçage logiciel tant que le bit de verrouillage correspondant n'a pas été défini. Une fois que le bit de verrouillage est défini, il n'est plus possible de modifier le bit d'amorçage logiciel ni le bit de verrouillage. Les bits d'amorçage logiciel et leurs bits de verrouillage correspondants sont réinitialisés au redémarrage du Secure Enclave.
BPR (Boot Progress Register), registre de progression du démarrage	Ensemble d'indicateurs matériels de puce-système que les logiciels peuvent utiliser pour effectuer le suivi des différents modes de démarrage utilisés par l'appareil, tels que le mode DFU ou le mode de récupération. Une fois activé, un indicateur BPR ne peut plus être désactivé. Cela permet à un logiciel de disposer par la suite d'un indicateur fiable de l'état du système.
Cartographie des angles des crêtes papillaires	Représentation mathématique du sens 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 (définie sur trois 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 : en incorporant l'UID ou PBKDF2, le salage et le nombre d'itérations. • Une liste de clés de classe : – UUID de clé ; – une classe (classe de protection des données de trousseau ou de fichier) ; – type d'enveloppe (clé dérivée de l'UID uniquement ; clé dérivée de l'UID et clé dérivée du code) ; – clé de classe enveloppée ; – clé publique pour les classes asymétriques.
Contrôleur de mémoire	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.
Data Protection (Protection des 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.

DFU (Device Firmware Upgrade), mise à niveau de logiciel interne d'appareil	Mode d'attente adopté par le code de la ROM de démarrage d'un appareil avant une récupération via 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. »
ECDHE (Elliptic Curve Diffie-Hellman Exchange), échange de clés Diffie-Hellman basé sur des courbes elliptiques	Échange Diffie-Hellman basé sur des courbes elliptiques faisant appel à des clés éphémères. L'échange ECDHE permet à deux parties de convenir d'une clé secrète d'une manière qui empêche toute découverte de la clé par un dispositif d'écoute ciblant les messages échangés entre les deux parties.
ECDSA	Algorithme de signature numérique basé sur la cryptographie sur courbes elliptiques.
ECID (Exclusive Chip Identification), identifiant unique de l'appareil	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 à travers iCloud est coupée par une brève publication via Bluetooth Low Energy 4.0. Les octets de cette publication sont chiffrés par le biais de la même méthode que les publications de type Handoff. Il est utilisé dans le cadre du processus de personnalisation et n'est pas considéré comme un secret.
Effaceable Storage (Stockage effaçable)	Zone dédiée de l'espace de stockage NAND, utilisée pour stocker des clés cryptographiques. 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.
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.
HSM (Hardware Security Module), module de sécurité matériel	Ordinateur spécialisé, protégé contre toute manipulation, utilisé pour sauvegarder et gérer des clés numériques.
iBoot	Code qui charge XNU, dans le cadre d'une chaîne de démarrage sécurisée. En fonction de la génération de puces-système, iBoot peut être chargé soit par LLB, soit directement par la ROM de démarrage.
Identifiant de groupe (GID)	Semblable à l'UID, mais commun à tous les processeurs d'une classe.
IDS (Apple identity service), service d'identité Apple	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.
JTAG (Joint Test Action Group)	Outil de débogage matériel standard utilisé par les programmeurs et les développeurs de circuits.
LLB (Low-Level Bootloader), chargeur de démarrage de bas niveau	Sur les systèmes dotés d'une architecture de démarrage en deux étapes, il s'agit du code invoqué par la ROM de démarrage, qui charge à son tour iBoot dans le cadre d'une chaîne de démarrage sécurisé.
Profil d'approvisionnement	Fichier plist signé par Apple, qui contient un ensemble d'entités et de droits 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.
Randomisation du format d'espace d'adresse (ASLR)	Technique utilisée par iOS pour rendre plus difficile l'exploitation d'un bug 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 ultérieur, la position de toutes les bibliothèques et apps système est déterminée de manière aléatoire, de même que celle des apps de tierce partie compilées en tant qu'exécutables indépendamment de la position.
ROM de démarrage (boot)	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.

SCIP (System Coprocessor Integrity Protection), protection de l'intégrité des coprocesseurs système	Les coprocesseurs système sont des unités centrales de traitement placées sur la même puce-système que le processeur d'application.
SoC (System on a chip), système sur puce	Circuit intégré (CI) incorporant plusieurs composants sur une seule puce. Le processeur d'application, Secure Enclave et les autres coprocesseurs sont des composants du SoC.
Tangling, emmêlement	Processus par lequel le code d'un utilisateur est transformé en clé cryptographique 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.
Trousseau	L'infrastructure et un ensemble d'API utilisés par iOS et les apps de tierce partie pour stocker et récupérer des mots de passe, des clés et d'autres informations d'identification sensibles.
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 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, le sandboxing, la vérification des droits et la distribution aléatoire de l'espace d'adressage (ASLR).

Historique des révisions du document

Date	Résumé
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 • Cartes Express avec réserve d'énergie • Mode de récupération et mode DFU • Accessoires de télécommande télé HomeKit • Cartes sans contact • Cartes d'étudiant • Suggestions 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 biométriques • HomeKit • Apple Pay • Discussions d'affaires • 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/Face ID • Notes partagées • Chiffrement de bout en bout de CloudKit • TLS • Apple Pay, effectuer des paiements avec Apple Pay sur le web • Suggestions Siri • iPad partagé Pour en savoir plus sur les correctifs de sécurité d'iOS 11, consultez : https://support.apple.com/HT208112

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 Pour en savoir plus sur les correctifs de sécurité d'iOS 10.3, consultez : https://support.apple.com/HT207617
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, effectuer des paiements avec Apple Pay sur le web • Transfert sur cartes bancaires et prépayées • Suggestions Safari Pour en savoir plus sur les correctifs de sécurité d'iOS 10, consultez : https://support.apple.com/HT207143
Mai 2016	**Actualisé pour iOS 9.3** • Identifiant Apple géré • Identification à deux facteurs pour l'identifiant Apple • Conteneurs de clés • Certifications de sécurité • Mode Perdu et Verrouillage d'activation • Notes sécurisées • Apple School Manager, iPad partagé Pour en savoir plus sur les correctifs de sécurité d'iOS 9.3, consultez : https://support.apple.com/HT206166

Date	Résumé
Septembre 2015	**Actualisé pour iOS 9** • Verrouillage d'activation de l'Apple Watch • Règlements inhérents aux codes • 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 d'émetteur de carte Apple Pay • Indexation Spotlight sur l'appareil • Modèle de jumelage iOS • Apple Configurator 2 • Restrictions Pour en savoir plus sur les correctifs de sécurité d'iOS 9, consultez : https://support.apple.com/HT205212

Novembre 2018