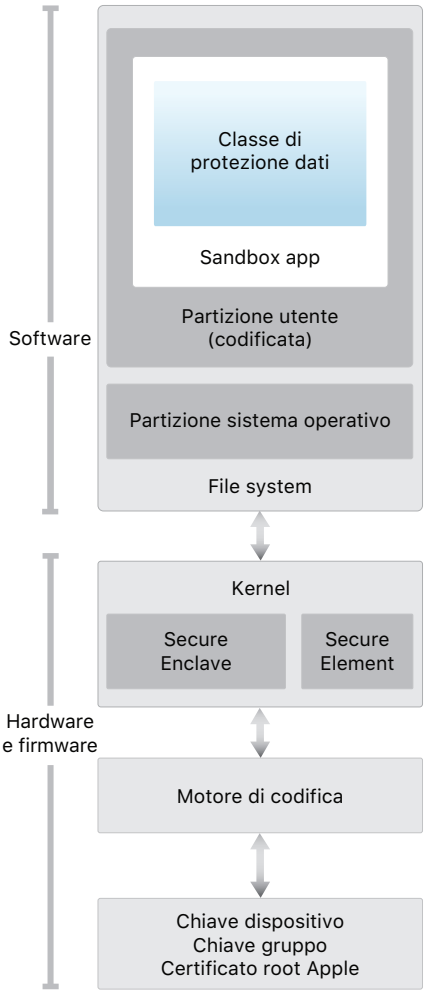
Sicurezza in iOS

iOS 12.1

Novembre 2018

Indice

Introduzione



Il diagramma dell'architettura di sicurezza di iOS fornisce una panoramica sulle varie tecnologie presentate in questo documento.

Apple ha progettato la piattaforma iOS dando massima priorità alla sicurezza. Quando ci siamo proposti di creare la miglior piattaforma mobile possibile, abbiamo attinto da decenni di esperienza e siamo stati in grado di realizzare un'architettura completamente nuova. Tenendo sempre a mente la vulnerabilità in materia di sicurezza dell'ambiente desktop, nella progettazione di iOS abbiamo optato per un nuovo approccio mirato a ottenere importanti miglioramenti in questo ambito. Abbiamo sviluppato e incorporato funzionalità innovative volte a rafforzare la sicurezza dei dispositivi mobili e a proteggere l'intero sistema di default. iOS rappresenta oggi un significativo passo in avanti in materia di sicurezza dei dispositivi mobili.

Ogni singolo dispositivo iOS unisce software, hardware e servizi progettati per lavorare insieme al fine di garantire la massima sicurezza e un'esperienza utente semplice e intuitiva. iOS non protegge solo il dispositivo e i dati in esso contenuti quando il sistema è a riposo, bensì protegge l'intero ecosistema, incluse tutte le operazioni che l'utente esegue localmente, su rete e con i principali servizi Internet.

iOS e i dispositivi iOS forniscono funzionalità di sicurezza avanzate pur mantenendo la facilità d'uso. Molte di queste funzionalità sono abilitate di default, di conseguenza l'integrazione dei dispositivi può avvenire senza alcun intervento da parte del reparto IT in quanto non sarà necessario eseguire configurazioni su larga scala. Inoltre, le funzionalità chiave relative alla sicurezza, come ad esempio la codifica del dispositivo, non sono configurabili e dunque gli utenti non potranno disabilitarle per errore. Altre funzionalità, come ad esempio Face ID, migliorano l'esperienza utente rendendo più semplice e intuitiva la protezione del dispositivo.

Il presente documento fornisce informazioni dettagliate su come la tecnologia e le funzionalità relative alla sicurezza sono implementate all'interno della piattaforma iOS. Sarà inoltre un valido strumento per la aziende che desiderano integrare la tecnologia e le funzionalità di sicurezza della piattaforma iOS nelle proprie politiche e procedure al fine di dare una risposta ai bisogni specifici in materia di sicurezza.

Il documento è organizzato per argomenti:

- **Sicurezza del sistema:** software e hardware sicuri e integrati che costituiscono la piattaforma per iPhone, iPad e iPod touch.
- **Codifica e protezione dati:** l'architettura e il design volti a proteggere i dati utente se il dispositivo viene smarrito o rubato, oppure se una persona non autorizzata prova a utilizzarlo o a modificarlo.
- **Sicurezza delle app:** sistemi che consentono di eseguire le app con la massima sicurezza senza compromettere l'integrità della piattaforma.
- **Sicurezza della rete:** protocolli di rete basati sugli standard del settore che forniscono autenticazione e codifica sicure durante la trasmissione dei dati.

- **Apple Pay:** implementazione Apple per i pagamenti sicuri.
- **Servizi Internet:** infrastruttura Apple di messaggeria, sincronizzazione e backup basata su rete.
- **Gestione delle password dell'utente:** restrizioni relative alla password e accesso alle password da altre fonti autorizzate.
- **Controlli del dispositivo:** metodi che consentono la gestione dei dispositivi iOS, impediscono l'uso non autorizzato e abilitano l'inizializzazione remota del dispositivo in caso di smarrimento o furto.
- **Controlli per la privacy:** funzionalità di iOS che possono essere utilizzate per controllare l'accesso ai servizi di localizzazione e ai dati dell'utente.
- **Certificazioni e programmi di sicurezza:** informazioni sulle certificazioni ISO, convalida crittografica, certificazione Common Criteria e CSfC (Commercial Solutions for Classified).

Sicurezza del sistema

Entrare in modalità DFU (Device Firmware Upgrade)

Il ripristino di un dispositivo in seguito all'attivazione della modalità DFU (detta anche modalità di recupero) consente di riportarlo a uno stato sicuramente funzionante, con la certezza che contenga solo codice firmato da Apple e non modificato. Non è possibile entrare manualmente in modalità DFU.

Per prima cosa, collega il dispositivo a un computer tramite un cavo USB.

Quindi, in base al dispositivo, esegui le seguenti operazioni:

iPhone X o modelli successivi, iPhone 8 o iPhone 8 Plus. Premi e rilascia rapidamente il tasto Volume su. Premi e rilascia rapidamente il tasto Volume giù. Tieni premuto il tasto laterale, quindi premi di nuovo il tasto Volume giù. Rilascia il tasto laterale dopo 5 secondi e continua a tenere premuto il tasto Volume giù finché non viene mostrata la schermata della modalità di recupero.

iPhone 7 o iPhone 7 Plus. Tieni premuti contemporaneamente il tasto laterale e il tasto Volume giù. Rilascia il tasto laterale e continua a tenere premuto il tasto Volume giù finché non viene mostrata la schermata della modalità di recupero.

iPhone 6s e modelli precedenti, iPad o iPod touch. Tieni premuti contemporaneamente il tasto Home e il tasto superiore (o laterale). Rilascia il tasto superiore (o laterale) e continua a tenere premuto il tasto Home finché non viene mostrata la schermata della modalità di recupero.

Nota: quando il dispositivo si trova in modalità DFU, sullo schermo non viene mostrato niente. Se viene mostrato il logo Apple, il tasto laterale o il tasto Standby/Riattiva sono stati premuti troppo a lungo.

La sicurezza del sistema è stata progettata in modo integrato affinché sia il software sia l'hardware siano sicuri in tutti i componenti principali di ogni singolo dispositivo iOS. Ne fanno parte la procedura di avvio, gli aggiornamenti software e Secure Enclave. Questa architettura occupa una posizione cardine nella sicurezza di iOS e non compromette mai la facilità d'uso del dispositivo.

La perfetta integrazione di hardware, software e servizi nei dispositivi iOS garantisce l'affidabilità di ogni componente del sistema e convalida il sistema a livello globale. Dall'avvio iniziale, agli aggiornamenti software iOS, fino ad arrivare alle app di terze parti, ogni singolo passo viene analizzato e vagliato per garantire l'interazione ottimale tra hardware e software e per garantire l'utilizzo corretto delle risorse.

Procedura di avvio sicuro

Ogni passo del processo di avvio contiene componenti che sono stati firmati digitalmente da Apple attraverso opportuna codifica per garantirne l'integrità e a cui viene consentito procedere solo dopo aver verificato la catena di affidabilità. Tale processo include i bootloader, il kernel, le estensioni del kernel e il firmware baseband. Questa procedura di avvio sicuro aiuta a garantire che i livelli più bassi del software non vengano alterati.

Quando un dispositivo iOS è acceso, il processore per le applicazioni esegue immediatamente il codice dalla memoria di sola lettura conosciuta come **ROM di avvio**. Questo codice immutabile, conosciuto come la radice di attendibilità dell'hardware, viene configurato durante la fabbricazione del chip ed è considerato implicitamente affidabile. Il codice della ROM di avvio contiene la chiave pubblica dell'autorità di certificazione root di Apple, utilizzata per verificare che il bootloader iBoot sia stato firmato da Apple prima di consentirne il caricamento. Questo è il primo passo della catena di affidabilità, in cui ogni passo garantisce che quello successivo sia firmato da Apple. Dopo aver concluso le proprie attività, iBoot controlla ed esegue il kernel iOS. Per i dispositivi con processori A9 o serie A precedenti, viene caricata una fase **bootloader di livello inferiore (LLB, Low-Level Bootloader)** che viene verificata dalla ROM di avvio e che a sua volta carica e verifica iBoot.

Se il caricamento di LLB (sui dispositivi meno recenti) o di iBoot (sui dispositivi più recenti) da parte della ROM di avvio non va a buon fine, il dispositivo entra in modalità DFU. Nel caso in cui LLB o iBoot non riescano a caricare o verificare il passaggio successivo, l'avvio viene arrestato e il dispositivo mostra la schermata "Collega a iTunes". Questa condizione è conosciuta come modalità di recupero. In entrambi i casi, è necessario collegare il dispositivo a iTunes tramite USB e ripristinare le impostazioni di fabbrica.

Il **registro di avanzamento dell'avvio (BPR, Boot Progress Register)** è utilizzato da Secure Enclave per limitare l'accesso ai dati dell'utente in diverse modalità e viene aggiornato prima di entrare nelle seguenti modalità:

- **Modalità di recupero:** impostata da iBoot sui dispositivi con processori Apple A10, S2 e **sistemi su circuito integrato (SoC, System on Chip)** più recenti.
- **Modalità DFU:** impostata dalla ROM di avvio sui dispositivi con SoC A12.

Per ulteriori informazioni, consulta la sezione "Codifica e protezione dati" di questo documento.

Sui dispositivi con accesso cellulare, anche il sottosistema baseband utilizza un processo di avvio sicuro simile, con software firmato e chiavi verificate dal processore baseband.

Anche il coprocessore Secure Enclave utilizza un processo di avvio sicuro che garantisce che il suo software separato sia verificato e firmato da Apple. Consulta la sezione "Secure Enclave" di questo documento.

Per ulteriori informazioni su come entrare manualmente in modalità di recupero, consulta: https://support.apple.com/HT1808

Autorizzazione software di sistema

Apple rilascia periodicamente aggiornamenti software volti a risolvere sul nascere eventuali problematiche di sicurezza e a fornire nuove funzionalità; gli aggiornamenti sono resi disponibili nello stesso momento per tutti i dispositivi. Gli utenti ricevono le notifiche sugli aggiornamenti di iOS sul dispositivo e attraverso iTunes; gli aggiornamenti vengono forniti in modalità wireless e ne viene consigliata l'installazione agli utenti sottolineando l'importanza dei miglioramenti apportati alla sicurezza.

Il processo di avvio descritto precedentemente aiuta a garantire che su un dispositivo possa essere installato solo codice firmato da Apple. Per evitare che i dispositivi possano venire riportati a versioni precedenti prive degli ultimi aggiornamenti di sicurezza, iOS utilizza un processo chiamato *autorizzazione software di sistema*. Se fosse possibile riportare il software a una versione precedente non più aggiornata, un malintenzionato che si fosse illegalmente impossessato del dispositivo potrebbe facilmente trarre vantaggio da un problema di vulnerabilità del sistema risolto in una versione più recente.

Su un dispositivo con Secure Enclave, il coprocessore Secure Enclave utilizza anche il processo di autorizzazione software di sistema per garantire l'integrità del software e impedire l'installazione di versioni non aggiornate. Consulta la sezione "Secure Enclave" di questo documento.

Gli aggiornamenti del software iOS possono essere installati tramite iTunes o in modalità wireless sul dispositivo. Con iTunes, viene scaricata e installata una copia completa di iOS. Gli aggiornamenti software in modalità wireless piuttosto che scaricare l'intero sistema operativo, scaricano solo i componenti richiesti per completare l'aggiornamento, migliorando così l'efficienza della rete. Inoltre, possono essere archiviati nella cache sui Mac con macOS High Sierra o versioni successive e su cui è abilitata la cache dei contenuti; in questo modo i dispositivi iOS non hanno bisogno di scaricare nuovamente gli aggiornamenti necessari da Internet. Tuttavia dovranno contattare i server Apple per completare il processo di aggiornamento.

Durante un aggiornamento iOS, iTunes (o il dispositivo stesso, se si tratta di aggiornamenti software in modalità wireless) si collega al server Apple di autorizzazione per l'installazione e invia a esso un elenco di misurazioni di codifica per ogni singola parte del pacchetto di installazione che deve essere installato (ad esempio iBoot, il kernel e l'immagine del sistema operativo), un valore anti-replay casuale (nonce) e **l'ID unico del chip del dispositivo (ECID)**.

Il server di autorizzazione verifica l'elenco di misurazioni che è stato presentato e lo paragona alle versioni in cui è stata permessa l'installazione; se trova una corrispondenza, aggiunge l'ECID alla misurazione e firma il risultato. Il server trasmette al dispositivo un set completo di dati firmati come parte del processo di aggiornamento. L'aggiunta dell'ECID "personalizza" l'autorizzazione per il dispositivo che la richiede. Autorizzando e firmando solo le misurazioni conosciute, il server assicura che l'aggiornamento avvenga esattamente secondo i parametri dettati da Apple.

La verifica tramite catena di fiducia al momento dell'avvio controlla che la firma provenga da Apple e che la misurazione dell'elemento caricato dal disco, unito all'ECID del dispositivo, corrispondano a ciò che è coperto dalla firma. Questi passaggi garantiscono che l'autorizzazione sia indirizzata a un dispositivo specifico e che una versione meno recente di iOS non possa essere copiata da un dispositivo a un altro. Il nonce serve a impedire che un pirata informatico possa salvare la risposta del server e che possa utilizzarla per danneggiare un dispositivo, oppure per alterare il software di sistema.

Secure Enclave

Secure Enclave è un coprocessore fabbricato all'interno del sistema su circuito integrato. Utilizza una memoria codificata e include un generatore hardware di numeri casuali. Secure Enclave fornisce tutte le operazioni codificate per la gestione della chiave di **protezione dei dati** e preserva l'integrità della protezione dei dati anche qualora sia stato compromesso il kernel. La comunicazione tra Secure Enclave e il processore per le applicazioni è isolata in una casella di posta guidata da interrupt (interrupt-driven) e in buffer di dati di memoria condivisa.

Secure Enclave include una ROM di avvio dedicata. Simile alla ROM di avvio del processore per le applicazioni, la ROM di avvio di Secure Enclave è costituita da codice immutabile che stabilisce la radice hardware della catena di fiducia per Secure Enclave.

Su Secure Enclave è in esecuzione un sistema operativo apposito basato su una versione personalizzata da Apple del microkernel L4. Il sistema operativo di Secure Enclave è firmato da Apple, verificato dalla ROM di avvio di Secure Enclave e aggiornato tramite una procedura di aggiornamento software personalizzata.

Quando il dispositivo si avvia, viene creata una chiave effimera di protezione della memoria dalla ROM di avvio di Secure Enclave; questa viene legata all'UID del dispositivo e utilizzata per codificare la porzione di Secure Enclave nello spazio di memoria del dispositivo. Fatta eccezione per il processore Apple A7, anche la memoria di Secure Enclave viene autenticata tramite la chiave di protezione della memoria. Su A11 e processori più recenti e sui SoC S4, viene utilizzato un albero di integrità che impedisce il riutilizzo di porzioni di memoria di Secure Enclave importanti a livello di sicurezza, autenticato dalla chiave di protezione della memoria e dai nonce archiviati nella SRAM integrata nel processore.

I dati salvati nel file system da Secure Enclave sono codificati con una chiave legata all'UID e con un contatore che ne impedisce il riutilizzo. Tale contatore è archiviato in un **circuito integrato** di memoria non volatile dedicato.

Sui dispositivi con A12 e Soc S4, Secure Enclave è abbinato a un circuito integrato di archiviazione sicura per l'archiviazione del contatore che impedisce il riutilizzo. Il circuito integrato di archiviazione sicura è progettato con un codice ROM immutabile, un generatore di numeri casuali hardware, motori crittografici e un sistema di rilevamento di manomissione fisica. Per leggere e aggiornare i contatori, Secure Enclave e il circuito integrato di archiviazione impiegano un protocollo sicuro che garantisce un accesso esclusivo ai contatori.

I servizi anti-riutilizzo su Secure Enclave sono usati per revocare i dati in caso di eventi considerati come limiti per il riutilizzo. Tali eventi includono:

- Modifica del codice.
- Abilitazione o disabilitazione di Touch ID o Face ID.
- Aggiunta o rimozione di impronte digitali.
- Ripristino di Face ID.
- Aggiunta o rimozione di carte Apple Pay.
- Inizializzazione dei contenuti e delle impostazioni.

Secure Enclave si occupa anche dell'elaborazione dei dati delle impronte digitali e dei dati facciali ottenuti dai sensori Touch ID e Face ID, stabilendo se esiste una corrispondenza e consentendo l'accesso o gli acquisti per conto dell'utente.

Protezione dell'integrità del sistema operativo

Protezione dell'integrità del kernel

Una volta che il kernel di iOS ha completato l'inizializzazione, la protezione dell'integrità del kernel viene abilitata per impedire modifiche al codice del kernel e dei driver. Il **controller della memoria** fornisce una regione di memoria fisica protetta che **iBoot** utilizza per caricare il kernel e le estensioni del kernel. Una volta completato l'avvio, il controller della memoria nega la scrittura sulla regione di memoria fisica protetta. Inoltre, l'unità di gestione della memoria del processore per le applicazioni è configurata in modo tale da impedire la mappatura di codice con privilegi dalla memoria fisica al di fuori dalla regione di memoria protetta e in modo tale da impedire mappature scrivibili della memoria fisica all'interno della regione di memoria del kernel.

L'hardware utilizzato per abilitare la protezione dell'integrità del kernel viene bloccato dopo il completamento della procedura di avvio per impedire la riconfigurazione. La protezione dell'integrità del kernel è supportata sui SoC Apple a partire da A10 e S4.

Protezione dell'integrità dei coprocessori di sistema

I coprocessori di sistema sono CPU sullo stesso SoC del processore per le applicazioni. I coprocessori di sistema sono dedicati a scopi specifici e il kernel di iOS delega a essi varie attività. Alcuni esempi sono:

- Secure Enclave
- Processore del sensore fotografico
- Coprocessore di movimento

Dal momento che il firmware del coprocessore gestisce molte attività critiche del sistema, la sua sicurezza è un fattore fondamentale per la sicurezza globale del sistema.

La protezione dell'integrità dei coprocessori di sistema utilizza un meccanismo simile alla protezione dell'integrità del kernel per impedire la modifica del firmware dei coprocessori. Durante l'avvio, iBoot carica il firmware di ciascun coprocessore in una regione di memoria protetta, riservata e separata dalla regione per la protezione dell'integrità del kernel. iBoot configura ciascuna unità di gestione della memoria dei coprocessori per impedire quanto segue:

- Mappature eseguibili al di fuori della parte di regione di memoria protetta.
- Mappature scrivibili all'interno della parte di regione di memoria protetta.

Il sistema operativo di Secure Enclave è responsabile della configurazione della protezione dell'integrità di Secure Enclave all'avvio.

L'hardware utilizzato per abilitare la protezione dell'integrità dei coprocessori di sistema viene bloccato dopo il completamento della procedura di avvio per impedire la riconfigurazione. La protezione dell'integrità dei coprocessori di sistema è supportata sui SoC a partire da A12 e S4.

Codici di autenticazione dei puntatori

I codici di autenticazione dei puntatori vengono utilizzati come protezione contro lo sfruttamento di bug che causano il danneggiamento della memoria. Il software di sistema e le app integrate utilizzano i codici di autenticazione dei puntatori per impedire la modifica dei puntatori delle funzioni e indirizzi di ritorno (puntatori del codice). Questo aumenta la difficoltà di molti attacchi. Ad esempio, un attacco basato sul return oriented programming tenta di ingannare il dispositivo in modo tale che esegua del codice in maniera dannosa manipolando gli indirizzi di ritorno delle funzioni archiviati sullo stack.

I codici di autenticazione dei puntatori sono supportati su A12 e sui SoC S4.

Touch ID

Touch ID è il sistema di rilevamento di impronte digitali che permette di accedere a iPhone e iPad in tutta sicurezza in modo semplice e veloce. Questa tecnologia legge i dati delle impronte digitali da qualsiasi angolazione e, nel tempo, impara a conoscerle sempre meglio; il sensore continua infatti ad ampliare la mappa dell'impronta perché con l'utilizzo vengono individuati nuovi nodi in sovrapposizione.

Face ID

Con un semplice sguardo, Face ID sblocca in tutta sicurezza i dispositivi Apple che ne sono dotati. Questa funzionalità fornisce un'autenticazione intuitiva e sicura resa possibile dal sistema fotografico TrueDepth, che utilizza tecnologie avanzate per eseguire una mappatura accurata della geometria del volto dell'utente. Face ID utilizza le reti neurali per determinare l'attenzione, stabilire la corrispondenza e impedire la falsificazione. Ciò ti consente di sbloccare il telefono con uno sguardo. Face ID si adatta automaticamente ai cambiamenti di aspetto e protegge accuratamente la privacy e la sicurezza dei dati biometrici dell'utente.

Touch ID, Face ID e codici

Per poter utilizzare Touch ID o Face ID, l'utente deve configurare il dispositivo in maniera tale che sia richiesto un codice per sbloccarlo. Quando Touch ID o Face ID rilevano una corrispondenza corretta, il dispositivo si sblocca senza chiedere l'inserimento del codice. In questo modo l'utilizzo di un codice più lungo e complesso diventa più pratico che mai, perché gli utenti non dovranno inserirlo spesso. Touch ID e Face ID non sostituiscono il codice, ma forniscono un accesso semplice al dispositivo entro limiti e soglie temporali appositamente pensate. Si tratta di un aspetto importante, perché un codice complesso costituisce le fondamenta della protezione crittografica dei tuoi dati da parte del dispositivo iOS.

Puoi utilizzare il codice in qualsiasi momento al posto di Touch ID o di Face ID, ma le seguenti operazioni richiedono sempre un codice al posto delle rilevazione biometriche:

- Aggiornamento del software.
- Inizializzazione del dispositivo.
- Visualizzazione o modifica delle impostazioni del codice.
- Installazione di profili di configurazione di iOS.

Il codice è richiesto anche se il dispositivo si trova in uno dei seguenti stati:

- Il dispositivo è stato appena acceso o riavviato.
- Il dispositivo non è stato sbloccato per più di 48 ore.
- Il codice non è stato usato per sbloccare il dispositivo nelle ultime 156 ore (sei giorni e mezzo) e una rilevazione biometrica non ha sbloccato il dispositivo nelle ultime 4 ore.
- Il dispositivo ha ricevuto un comando di blocco remoto.
- Dopo cinque tentativi di corrispondenza non riusciti tramite rilevazioni biometriche.
- Dopo uno spegnimento o dopo l'utilizzo di “SOS emergenze”.

Quando Touch ID o Face ID sono abilitati, il dispositivo si blocca immediatamente quando viene premuto il tasto laterale e ogni volta che entra in standby. Touch ID e Face ID richiedono una corrispondenza corretta (o facoltativamente il codice) a ogni riattivazione.

La probabilità che una persona casuale nella popolazione possa sbloccare iPhone è 1 su 50.000 con Touch ID o 1 su 1.000.000 con Face ID. Questa probabilità diminuisce se si registrano più impronte digitali (fino a 1 su 10.000 con cinque impronte digitali) o più fisionomie (fino a 1 su 500.000 con due fisionomie). Come forma di protezione ulteriore, sia Touch ID che Face ID consentono solo cinque tentativi di riconoscimento non riusciti prima di richiedere un codice per consentire l'accesso al

dispositivo. Con Face ID, la probabilità di un falso riconoscimento è diversa per i gemelli e per i fratelli o sorelle che si somigliano e per i bambini di età inferiore ai 13 anni, dal momento che le loro caratteristiche facciali distintive potrebbero non essersi ancora del tutto sviluppate. Se questo punto è fonte di preoccupazione, Apple consiglia di utilizzare un codice per l'autenticazione.

Sicurezza di Touch ID

Il sensore di impronte è attivo solo quando l'anello in acciaio capacitivo che circonda il tasto Home rileva il tocco di un dito. Questa operazione attiva la scansione avanzata dell'immagine del dito e la invia a Secure Enclave. La comunicazione tra il processore e il sensore Touch ID avviene tramite bus SPI (Serial Peripheral Interface). Il processore si occupa di trasmettere i dati a Secure Enclave ma non può leggerli, perché sono codificati e autenticati con una chiave di sessione negoziata tramite una chiave condivisa fornita a ogni sensore Touch ID e al Secure Enclave corrispondente durante la fabbricazione. La chiave condivisa è complessa, casuale e diversa per ogni sensore Touch ID. Lo scambio di chiave di sessione utilizza la **cifratura della chiave** AES, un processo in cui entrambe le parti forniscono una chiave casuale che stabilisce la chiave di sessione e utilizza la codifica di trasporto dati AES-CCM.

La scansione raster viene temporaneamente archiviata nella memoria codificata all'interno di Secure Enclave mentre viene vettorializzata per l'analisi e successivamente viene eliminata. L'analisi utilizza la **mappatura angolare del disegno papillare** dello strato sottocutaneo del dito, un processo con perdita che scarta i dettagli particolari, cioè le caratteristiche che sarebbero richieste per ricostruire l'impronta reale dell'utente. La mappa risultante di nodi è registrata, senza alcun tipo di informazione relativa all'identità, in un formato codificato che può essere letto solo da Secure Enclave. Questi dati non escono mai dal dispositivo: non vengono inviati ad Apple e non vengono inclusi nei backup del dispositivo.

Sicurezza di Face ID

Face ID è una funzionalità progettata per confermare la presenza di attenzione da parte dell'utente, fornire un solido metodo di autenticazione con basse probabilità di errato riconoscimento e ridurre la possibilità di falsificazione, sia digitale che fisica.

La fotocamera TrueDepth inquadra automaticamente il volto quando l'utente riattiva un dispositivo Apple dotato di Face ID sollevandolo o toccando lo schermo, così come quando il dispositivo tenta di autenticare l'utente per mostrare una notifica in entrata oppure quando un'app supportata richiede l'autenticazione tramite Face ID. Quando Face ID rileva un volto, conferma la presenza di attenzione e l'intenzione di eseguire lo sblocco verificando che gli occhi siano aperti e l'attenzione sia rivolta verso il dispositivo; per questioni di accessibilità, questa condizione è disabilitata quando VoiceOver è attivato e, se richiesto, può essere disabilitata separatamente.

Una volta confermata la presenza di un volto attento, la fotocamera TrueDepth proietta e legge più di 30.000 punti ad infrarossi per formare una mappa di profondità del viso, insieme a un'immagine a infrarossi 2D. Tali dati vengono utilizzati per creare una sequenza di immagini 2D e di mappe di profondità, che vengono firmate digitalmente e inviate a Secure Enclave. Per contrastare la falsificazione sia fisica che digitale, la fotocamera TrueDepth rende casuale la sequenza delle immagini 2D e delle mappe di profondità e proietta un motivo casuale specifico per

ogni dispositivo. Una porzione del processore neurale di A11 e dei SoC più recenti, protetta all'interno di Secure Enclave, trasforma questi dati in una rappresentazione matematica e la confronta con i dati facciali registrati, che sono a loro volta una rappresentazione matematica del volto dell'utente, rilevato in varie pose.

Il riconoscimento facciale viene eseguito all'interno di Secure Enclave tramite reti neurali preparate appositamente per tale scopo. Abbiamo sviluppato le reti neurali per il riconoscimento facciale utilizzando oltre un miliardo di immagini, comprese immagini ad infrarossi e immagini 3D, raccolte in studi condotti con il consenso informato dei partecipanti. Apple ha lavorato con partecipanti di tutto il mondo per includere un gruppo rappresentativo di individui tenendo in considerazione genere, età, etnia e altri fattori. Gli studi sono stati appositamente ampliati per fornire un alto grado di precisione per una ricca varietà di utenti. Face ID è progettato per funzionare con cappelli, sciarpe, occhiali, lenti a contatto e molti occhiali da sole, nonché per funzionare al chiuso, all'aperto e persino totalmente al buio. Una rete neurale aggiuntiva, preparata per individuare e impedire la falsificazione, protegge contro i tentativi di sbloccare iPhone X con foto o maschere.

I dati di Face ID, comprese le rappresentazioni matematiche del volto dell'utente, sono codificate e disponibili solo per Secure Enclave. Questi dati non escono mai dal dispositivo: non vengono inviati ad Apple e non vengono inclusi nei backup del dispositivo. I dati di Face ID salvati e codificati per l'utilizzo esclusivo da parte di Secure Enclave durante il normale funzionamento sono i seguenti:

- Le rappresentazioni matematiche del volto calcolate durante la registrazione.
- Le rappresentazioni matematiche del volto calcolate durante alcuni tentativi di sblocco se Face ID le reputa utili a migliorare i riconoscimenti futuri.

Le immagini del volto rilevate durante il normale funzionamento non vengono salvate e vengono immediatamente eliminate una volta che le rappresentazioni matematiche sono calcolate per la registrazione o per il confronto con i dati di Face ID registrati.

Come avviene lo sblocco del dispositivo iOS da parte di Touch ID o Face ID

Con Touch ID o Face ID disabilitati, quando un dispositivo si blocca, le chiavi per la classe più alta della protezione dati (archiviate in Secure Enclave) vengono eliminate. I file e gli elementi del **portachiavi** di quella classe non sono accessibili finché l'utente non sblocca il dispositivo inserendo il codice.

Con Touch ID o Face ID abilitati, le chiavi non vengono eliminate quando il dispositivo si blocca; sono invece cifrate tramite una chiave che viene fornita al sottosistema Touch ID o Face ID all'interno di Secure Enclave. Quando un utente prova a sbloccare il dispositivo, se il dispositivo rileva una corrispondenza corretta, fornirà la chiave per decifrare le chiavi di protezione dati e sarà dunque sbloccato. Questo processo fornisce un'ulteriore protezione perché richiede la cooperazione tra i sottosistemi della protezione dati e di Touch ID o Face ID per sbloccare il dispositivo.

Quando il dispositivo viene riavviato, le chiavi richieste per sbloccarlo tramite Touch ID o Face ID vengono perse: vengono eliminate da Secure Enclave ogni volta che si verifica una qualsiasi delle condizioni che richiedono l'inserimento del codice, come ad esempio, se il dispositivo non viene sbloccato per 48 ore o dopo cinque tentativi di riconoscimento non riusciti.

Per migliorare le prestazioni dello sblocco e restare al passo con i cambiamenti naturali del volto dell'utente, con il tempo Face ID incrementa le rappresentazioni matematiche archiviate. In seguito a uno sblocco riuscito, Face ID potrebbe utilizzare le rappresentazioni matematiche appena calcolate (se la qualità è sufficiente) per un numero finito di altri sblocchi, per poi eliminare tali dati. Se invece Face ID non riesce a riconoscere l'utente, ma la qualità del riconoscimento è più alta di una determinata soglia e subito dopo viene inserito il codice, Face ID esegue un'altra rilevazione e incrementa i dati di Face ID registrati con la rappresentazione matematica appena calcolata. Questi nuovi dati di Face ID vengono eliminati se non vengono più utilizzati per il riconoscimento e dopo un numero finito di sblocchi. Questo processo di incremento consente a Face ID di tenere il passo con cambiamenti importanti nei peli facciali o nell'utilizzo del trucco, minimizzando al tempo stesso i riconoscimenti errati.

Touch ID, Face ID e Apple Pay

È possibile utilizzare Touch ID e Face ID anche con Apple Pay per effettuare acquisti facili e sicuri in negozi, app e sul web. Per ulteriori informazioni su Touch ID e Apple Pay, consulta la sezione dedicata ad Apple Pay in questo documento.

Per autorizzare un pagamento in un negozio con Face ID, l'utente dovrà prima confermare l'intenzione di pagare facendo doppio clic con il tasto laterale. Quindi si eseguirà l'autenticazione con Face ID prima di posizionare iPhone X vicino al lettore per il pagamento contactless. Se l'utente vuole selezionare un metodo di pagamento diverso per Apple Pay dopo l'autenticazione con Face ID, dovrà effettuare di nuovo l'autenticazione, ma non dovrà fare doppio clic con il tasto laterale.

Per effettuare un pagamento all'interno delle app e sul web, l'utente conferma l'intenzione di pagare facendo doppio clic con il tasto laterale, quindi eseguirà l'autenticazione con Face ID per autorizzare il pagamento. Se la transazione di Apple Pay non viene completata entro 30 secondi dal momento in cui l'utente ha fatto doppio clic con il tasto laterale, occorrerà confermare l'intenzione di pagare facendo di nuovo doppio clic.

Diagnosi di Face ID

I dati di Face ID non escono mai dal dispositivo e non vengono mai inclusi nei backup su iCloud o in qualsiasi altra posizione. Tali informazioni vengono prelevate dal dispositivo solo nel caso in cui l'utente desideri fornire i dati di diagnosi di Face ID ad AppleCare per richiedere assistenza. L'abilitazione della diagnosi di Face ID richiede un'autorizzazione firmata digitalmente da Apple, simile a quella utilizzata per il processo personalizzato di aggiornamento del software. Dopo l'autorizzazione, l'utente potrà attivare la diagnosi di Face ID e iniziare il processo di configurazione all'interno dell'app Impostazioni sui dispositivi che supportano Face ID.

Come parte della configurazione della diagnosi di Face ID, la registrazione esistente verrà eliminata e verrà chiesto all'utente di eseguirla nuovamente. Sui dispositivi che supportano Face ID, verrà avviata la registrazione delle immagini di Face ID rilevate durante i tentativi di autenticazione per i 10 giorni successivi; dopo questo periodo di tempo, il salvataggio delle immagini verrà interrotto automaticamente. La diagnosi di Face ID non invia automaticamente dati ad Apple. Puoi controllare e approvare la registrazione e sbloccare le immagini (sia quelle con cui l'autenticazione è riuscita che quelle con cui non è riuscita) incluse nei dati di diagnosi di Face ID raccolti in modalità di diagnosi prima che vengono inviati ad Apple. La diagnosi di Face ID caricherà solo le immagini di diagnosi che hai approvato. I dati vengono codificati prima del caricamento e vengono immediatamente eliminati dal dispositivo una volta che il caricamento è completato. Le immagini rifiutate dall'utente vengono eliminate immediatamente.

Se l'utente non conclude la sessione di diagnosi di Face ID rivedendo le immagini e caricando quelle approvate, la diagnosi di Face ID terminerà automaticamente dopo 40 giorni e tutte le relative immagini verranno eliminate dal dispositivo. Inoltre è possibile disabilitare la diagnosi di Face ID in qualsiasi momento. In questo caso verranno eliminate immediatamente tutte le immagini locali e non verrà condiviso con Apple nessun dato di Face ID.

Altri usi di Touch ID e Face ID

Le app di terze parti possono utilizzare le API fornite dal sistema per richiedere l'autenticazione dell'utente tramite Touch ID, Face ID o un codice; le app compatibili con Touch ID, supportano automaticamente anche Face ID senza alcun cambiamento. Quando vengono utilizzati Touch ID o Face ID, all'app viene notificata solo l'avvenuta autenticazione: non potrà accedere a Touch ID, a Face ID né ad altri dati associati all'utente registrato. Anche gli elementi del portachiavi possono essere protetti con Touch ID o Face ID e saranno sbloccati da Secure Enclave solo con una corrispondenza corretta o utilizzando il codice del dispositivo. Gli sviluppatori di app dispongono di API per verificare che l'utente abbia impostato un codice prima di richiedere l'uso di Touch ID, Face ID o di un codice per sbloccare gli elementi del portachiavi. Gli sviluppatori di app possono:

- Impedire che le operazioni dell'API di autenticazione ricorrano alla password di un'app o al codice del dispositivo. Verificare che un utente sia registrato, consentendo l'utilizzo di Touch ID o Face ID come secondo fattore in app sensibili alla sicurezza.
- Generare e utilizzare chiavi ECC all'interno di Secure Enclave che possono essere protette da Touch ID o Face ID. Le operazioni con queste chiavi avvengono sempre all'interno di Secure Enclave dopo che Secure Enclave ne ha autorizzato l'uso.

Touch ID o Face ID possono anche essere configurati per l'approvazione degli acquisti su iTunes Store, App Store e Apple Books, così l'utente non dovrà inserire la password dell'ID Apple. Con iOS 11 o versione successiva, le chiavi ECC di Secure Enclave protette tramite Touch ID o Face ID vengono utilizzate per autorizzare un acquisto firmando la richiesta dello Store.

Codifica e protezione dati

Inizializzazione di contenuto e impostazioni
L'opzione “Inizializza contenuto e impostazioni” in Impostazioni elimina tutte le chiavi nella Effaceable Storage, codificando tutti i dati dell'utente sul dispositivo e rendendoli quindi illeggibili. È quindi una soluzione ideale per assicurarsi che le informazioni personali vengano rimosse dal dispositivo prima di assegnarlo ad altri o di mandarlo in assistenza.

Importante: non utilizzare l'opzione “Inizializza contenuto e impostazioni” senza prima effettuare un backup del dispositivo, in quanto non c'è modo di recuperare i dati cancellati.

La procedura di avvio sicuro, la firma del codice e la sicurezza del processo di runtime contribuiscono a garantire che solo il codice e le app affidabili possano venire eseguiti su un dispositivo. iOS dispone di funzionalità aggiuntive di codifica e protezione dati volte a salvaguardare i dati dell'utente, anche quando sono state compromesse altre parti dell'infrastruttura di sicurezza (ad esempio su un dispositivo con modifiche non autorizzate). Ciò apporta importanti benefici sia agli utenti che agli amministratori IT, in quanto fornisce protezione completa di tutte le informazioni aziendali e personali e metodi per la cancellazione immediata e totale a distanza in caso di furto o smarrimento del dispositivo.

Caratteristiche di sicurezza hardware

Sui dispositivi mobili, velocità ed efficienza sono punti cardine. Le operazioni di codifica sono complesse e possono causare problemi a livello di prestazioni o di durata della batteria se non sono progettate e implementate tenendo sempre a mente queste priorità.

Ogni dispositivo iOS possiede al suo interno un motore di codifica dedicato basato su AES-256, integrato nel percorso DMA tra la memoria flash e la memoria principale del sistema, rendendo altamente efficiente il processo di codifica dei file. Sui processori A9 o serie A successive, il sottosistema di archiviazione flash si trova su un bus isolato, che ha accesso alla memoria con i dati dell'utente unicamente mediante il motore di codifica del DMA.

Gli ID unici **del dispositivo (UID)** e gli ID di un gruppo **di dispositivi (GID)** sono chiavi AES a 256 bit fuse (UID) o compilate (GID) durante la fabbricazione all'interno del processore per le applicazioni e del Secure Enclave. Nessun software o firmware può leggerle direttamente; possono solo vedere i risultati delle operazioni di codifica o decodifica eseguite dai motori AES dedicati implementati su silicio, utilizzando l'UID o il GID come chiave. Il processore per le applicazioni e Secure Enclave hanno ciascuno il proprio UID e GID. L'UID e il GID di Secure Enclave possono essere utilizzati solo dal motore AES dedicato a Secure Enclave. Gli UID e i GID non sono inoltre disponibili via **JTAG (Joint Test Action Group)** o altre interfacce di debug.

Ad eccezione di Apple A8 e dei SoC precedenti, ciascun Secure Enclave genera il proprio UID durante il processo di produzione. Dato che l'UID è unico per ciascun dispositivo e dato che viene generato interamente all'interno di Secure Enclave piuttosto che in un sistema di produzione esterno al dispositivo, non è disponibile per l'accesso o l'archiviazione da parte di Apple o di qualsiasi suo fornitore.

Il software in esecuzione su Secure Enclave sfrutta l'UID per proteggere le informazioni segrete specifiche per il dispositivo. L'UID consente di collegare attraverso la codifica i dati a un dispositivo particolare. Ad esempio, la gerarchia di chiavi che protegge il file system include l'UID, quindi se i chip di memoria vengono fisicamente spostati da un dispositivo all'altro, i file sono inaccessibili. L'UID non è collegato a nessun altro identificatore sul dispositivo.

Il GID è comune a tutti i processori in una classe di dispositivi (ad esempio, tutti i dispositivi con processore Apple A8).

Fatta eccezione per UID e GID, tutte le altre chiavi di codifica sono create dal generatore di numeri casuali del sistema (RNG) utilizzando un algoritmo basato su codice sorgente CTR_DRBG. L'entropia del sistema è generata dalle variazioni temporali durante l'avvio e anche dai tempi di interrupt dopo che il dispositivo è stato avviato. Le chiavi generate all'interno di Secure Enclave utilizzano il proprio generatore hardware di numeri casuali basato su oscillatori ad anello multipli processati posteriormente con CTR_DRBG.

Eliminare in modo sicuro le chiavi salvate è importante tanto quanto generarle. L'eliminazione di tali chiavi risulta particolarmente difficile nella memoria flash, poiché ad esempio, a causa del livellamento dell'usura, potrebbe contenere più copie di dati da cancellare. Per risolvere questo problema, i dispositivi iOS includono una funzionalità dedicata alla cancellazione sicura dai dati chiamata **Effaceable Storage**. Tale funzionalità accede alla tecnologia di archiviazione sottostante (ad esempio, NAND) per concentrarsi direttamente su un numero ridotto di blocchi a un livello molto basso e cancellarli.

Modalità rapida delle carte in modalità "Basso consumo"

Se iOS non è in esecuzione perché iPhone necessita di essere caricato, potrebbe esserci energia sufficiente nella batteria per supportare le transazioni in modalità rapida.

Gli iPhone supportati supportano automaticamente questa funzionalità con:

- Una carta dei mezzi pubblici designata come carta rapida.
- Tessere identificative studente con la modalità rapida attivata.

Premendo il tasto laterale, viene mostrata l'icona della batteria scarica, insieme al testo che indica che le carte rapide sono disponibili per l'utilizzo. Il controller NFC esegue le transazioni in modalità rapida sotto le stesse condizioni quando iOS è in esecuzione, tranne per il fatto che le transazioni sono indicate solo con una notifica aptica. Non viene mostrata alcuna notifica visibile.

Questa funzionalità non è disponibile quando viene eseguito uno spegnimento standard da parte dell'utente.

Protezione dati dei file

Oltre alle funzionalità di codifica hardware integrate nei dispositivi iOS, Apple usa una tecnologia chiamata Protezione dati per proteggere ulteriormente i dati archiviati nella memoria flash sul dispositivo. La protezione dati consente al dispositivo di rispondere a eventi comuni quali le chiamate in entrata, ma abilita anche un alto livello di codifica per i dati utente. Le app chiave del sistema, quali Messaggi, Mail, Calendario, Contatti, Foto e i valori dei dati di Salute utilizzano di default la protezione dati e le app di terze parti installate su iOS 7 o versione successiva ricevono questa protezione automaticamente.

La protezione dati è implementata creando e gestendo una gerarchia di chiavi e costruisce sull'hardware tecnologie di codifica integrate in ogni singolo dispositivo iOS. La protezione dati è controllata per ogni singolo file e assegna a ognuno di essi una classe; l'accessibilità dei file dipende dallo stato, sbloccato o meno, delle chiavi della classe a cui appartengono.

Con l'introduzione di Apple File System (APFS), il file system è ora in grado di suddividere ulteriormente le chiavi per "entità", in maniera tale che porzioni diverse di un file possano avere chiavi diverse.

Panoramica sull'architettura

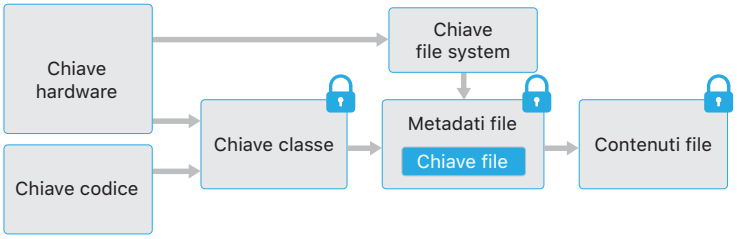
Ogni volta che viene creato un file sulla partizione dati, la protezione dati crea una nuova chiave a 256 bit (la chiave "per file") e la consegna al motore AES hardware, che utilizza la chiave per codificare il file mentre viene scritto nella memoria flash utilizzando la modalità AES-XTS. Sui dispositivi con SoC A7, S2 o S3, viene usata la modalità AES-CBC. Il vettore di inizializzazione è calcolato con il block offset nel file, codificato con l'hash SHA-1 della **chiave per file**.

La chiave per file (o per entità) è cifrata con una delle diverse chiavi di classe, a seconda delle circostanze in base alle quali il file deve essere accessibile. Proprio come tutti gli altri metodi di cifratura, viene eseguito utilizzando la cifratura NIST AES, come da RFC 3394. La chiave per file cifrata è memorizzata nei metadati del file.

I dispositivi che utilizzano il formato Apple File System possono supportare la clonazione dei file (copie a costo zero utilizzando la tecnologia di copia su scrittura). Se un file viene clonato, ciascuna metà del clone ottiene una nuova chiave per accettare le scritture in arrivo, in modo tale che i nuovi dati vengano scritti sul supporto con una nuova chiave. Con il tempo, il file può diventare composto da varie entità (o frammenti), ognuna associata a una chiave diversa. Tuttavia, tutte le entità che compongono un file verranno protette dalla stessa chiave di classe.

Quando viene aperto un file, i suoi metadati sono decodificati con la **chiave del file system**, rivelando la chiave per file cifrata e una nota sulla classe che la protegge. La cifratura della chiave per file (o per entità) viene tolta con la chiave di classe, quindi fornita al motore AES hardware che a sua volta decodifica il file mentre viene letto dalla memoria flash. La gestione delle chiavi dei file cifrate avviene interamente in Secure Enclave; la chiave per i file non viene mai esposta direttamente al processore per le applicazioni. All'avvio, Secure Enclave negozia una chiave effimera con il motore AES. Quando Secure Enclave rimuove la cifratura dalle chiavi di un file, queste vengono di nuovo cifrate con la chiave effimera e inviate di nuovo al processore per le applicazioni.

I metadati di tutti i file nel file system sono codificati con una chiave casuale, creata quando iOS viene installato per la prima volta o quando il dispositivo viene cancellato dall'utente. Sui dispositivi che supportano Apple File System, la chiave dei metadati del file system viene cifrata dalla chiave UID di Secure Enclave per l'archiviazione a lungo termine. Proprio come avviene per le chiavi per file o per entità, la chiave dei metadati non viene mai esposta direttamente al processore per le applicazioni; Secure Enclave ne fornisce invece una versione effimera diversa a ogni avvio. Quando viene archiviata, la chiave codificata del file system viene ulteriormente cifrata da una chiave effimera archiviata in Effaceable Storage. Tale chiave non è utilizzata per garantire la riservatezza dei dati. È piuttosto stata progettata per poter essere cancellata velocemente su richiesta (dall'utente, tramite l'opzione "Inizializza contenuto e impostazioni", oppure da un utente o un amministratore, inviando il comando di inizializzazione da remoto da una soluzione MDM, Exchange ActiveSync o iCloud). La cancellazione della chiave secondo questa modalità rende tutti i file inaccessibili a causa della codifica.



Il contenuto di un file può essere codificato con una o più chiavi per file (o per entità), cifrate con una chiave di classe e archiviata nei metadati di un file, a sua volta codificato con la chiave del file system. La chiave di classe è protetta con l'UID dell'hardware e, per alcune classi, con il codice dell'utente. Questa gerarchia fornisce flessibilità e prestazioni ottimali. Ad esempio, per modificare la classe di un file occorre solo cifrare nuovamente la sua chiave per file; la modifica del codice cifra di nuovo la chiave di classe.

Codici

Configurando un codice per il dispositivo, l'utente abilita automaticamente la protezione dei dati. iOS supporta codici a sei cifre, a quattro cifre e codici alfanumerici di qualunque lunghezza. Oltre a sbloccare il dispositivo, un codice fornisce entropia per determinate chiavi di codifica. Ciò significa che un pirata informatico in possesso di un dispositivo non potrà accedere ai dati conservati in classi di protezione specifiche senza il codice.

Considerazioni sul codice
Se viene inserita una password lunga che contiene solo numeri, in "Blocco schermo" compare un tastierino numerico anziché la tastiera completa. Un codice numerico lungo può essere più facile da inserire rispetto a un codice alfanumerico breve, pur fornendo un livello di sicurezza equivalente.

Il codice è legato all'UID del dispositivo, quindi è necessario eseguire un attacco di forza bruta, che deve essere realizzato sul dispositivo stesso. Il numero di iterazioni è calibrato in modo da far durare ogni tentativo circa 80 millisecondi. Questo significa che ci vorrebbero più di cinque anni e mezzo per provare tutte le combinazioni di un codice alfanumerico a sei caratteri.

Ritardi tra i tentativi di inserimento del codice

Tentativi	Ritardo forzato
1–4	Nessuno
5	1 minuto
6	5 minuti
7–8	15 minuti
9	1 ora

Quanto più è sicuro il codice impostato dall'utente, tanto più diventa sicura la chiave di codifica. Touch ID e Face ID possono essere utilizzati per migliorare questa equazione consentendo all'utente di stabilire un codice molto più sicuro che altrimenti non sarebbe pratico. In questo modo si mira a ottenere la più alta entropia possibile con l'obiettivo di proteggere le chiavi di codifica utilizzate per la protezione dati, senza influire negativamente sulla praticità di utilizzo da parte dell'utente che si trova a sbloccare il dispositivo iOS svariate volte durante la giornata.

Per dissuadere ulteriormente eventuali pirati informatici dal tentare di decifrare i codici, vengono applicati ritardi sempre più lunghi dopo l'inserimento di un codice errato in "Blocco schermo". Se Impostazioni > Touch ID e codice > Inizializza dati è attivato, il dispositivo verrà cancellato automaticamente dopo 10 tentativi errati consecutivi di inserimento del codice. Tentativi consecutivi con lo stesso codice errato non vengono conteggiati per il raggiungimento del limite. Questa impostazione è anche disponibile come politica amministrativa tramite una soluzione MDM che la supporti e Exchange ActiveSync, e può essere impostata su una soglia più bassa.

Sui dispositivi con Secure Enclave, i ritardi sono comandati dal coprocessore Secure Enclave. Se il dispositivo viene riavviato durante un ritardo, tale ritardo viene comunque applicato e il timer comincia da capo con l'intervallo attualmente in corso.

Per migliorare la sicurezza mantenendo l'usabilità, iOS 11.4.1 o versione successiva richiede Touch ID, Face ID o il codice per attivare l'interfaccia USB se USB non è stato utilizzato di recente. Questo elimina la possibilità di attacco per mezzo di dispositivi collegati fisicamente come caricatori dannosi, permettendo al tempo stesso di utilizzare gli accessori USB entro limiti di tempo ragionevoli. Se è trascorsa più di un'ora da quando il dispositivo iOS è stato bloccato o da quando è stato scollegato un collegamento USB, il dispositivo non consentirà nuovi collegamenti finché non viene sbloccato. Questo periodo di un'ora:

- Assicura che gli utenti che si collegano frequentemente a un Mac o a un PC, ad accessori USB o a CarPlay tramite cavo non debbano inserire il codice ogni volta che collegano i propri dispositivi.
- È necessario, perché l'ecosistema dell'accessorio USB non fornisce un metodo affidabile di identificazione dell'accessorio stesso prima di aver stabilito un collegamento dati.

Inoltre, su iOS 12, se sono trascorsi più di tre giorni dall'ultima volta che è stato stabilito un collegamento USB, il dispositivo impedirà nuovi collegamenti USB subito dopo il blocco. Ciò serve ad aumentare la protezione per gli utenti che non utilizzano tali collegamenti frequentemente. I collegamenti USB sono disabilitati anche nelle situazioni in cui il dispositivo si trova in uno stato che richiede un codice per riabilitare l'autenticazione tramite rilevamenti biometrici.

L'utente può scegliere di avere i collegamenti USB sempre attivi in Impostazioni; se viene configurato un dispositivo assistivo, l'opzione viene abilitata automaticamente.

Modalità DFU e di recupero

Sui dispositivi con SoC Apple A10, A11 e S3, non è possibile accedere dalla modalità di recupero alle chiavi di classe protette dal codice dell'utente. I SoC A12 e S4 estendono questa protezione anche alla modalità DFU.

Il motore AES di Secure Enclave è dotato di bit seed software bloccabili. Quando le chiavi vengono create dall'UID, questi bit seed vengono inclusi nella funzione di derivazione della chiave per creare gerarchie di chiave aggiuntive.

A partire dai SoC Apple A10 e S3, un bit seed è dedicato a distinguere le chiavi protette dal codice dell'utente. Il bit seed è impostato per le chiavi che richiedono il codice dell'utente (incluse le chiavi per la classe di protezione dati A, B e C), mentre viene eliminato per le chiavi che non richiedono il codice dell'utente (inclusa la chiave per i metadati del file system e le chiavi per la classe D).

Sul processore A12, la ROM di avvio di Secure Enclave blocca il bit seed del codice se il processore per le applicazioni è entrato in modalità DFU o di recupero. Quando il bit seed del codice è bloccato, non è consentita nessuna operazione di modifica, impedendo l'accesso ai dati protetti dal codice dell'utente.

Sui processori Apple A12, A11, S3 e S4, il bit seed del codice è bloccato dal sistema operativo di Secure Enclave se il dispositivo è entrato in modalità di recupero. Sia la ROM di avvio sia il sistema operativo di Secure Enclave controllano il registro di avanzamento dell'avvio per determinare la modalità attuale.

Classi di protezione dati

Quando viene creato un file nuovo su un dispositivo iOS, a esso viene assegnata una classe dall'app che l'ha creato. Ogni classe utilizza diverse politiche che stabiliscono quando i dati sono accessibili. Le classi e le politiche di base sono descritte nelle sezioni seguenti.

Protezione completa

(`NSFileProtectionComplete`): la chiave di classe è protetta da una chiave derivata dal codice utente e dall'UID del dispositivo. Poco dopo che l'utente ha bloccato il dispositivo (10 secondi se l'opzione "Richiedi password" è impostata su Subito), la classe decodificata viene eliminata, rendendo tutti i dati in essa contenuti inaccessibili finché l'utente non inserisce di nuovo il codice o sblocca il dispositivo tramite Touch ID o Face ID.

Protetto se non è aperto

(`NSFileProtectionCompleteUnlessOpen`): alcuni file potrebbero dover essere scritti mentre il dispositivo è bloccato, come ad esempio nel caso di un allegato e-mail che viene scaricato in background. Questo comportamento si ottiene utilizzando una codifica a curva ellittica asimmetrica (ECDH su Curve25519). La normale chiave per file è protetta da una chiave generata tramite il protocollo One-Pass Diffie-Hellman, come descritto in NIST SP 800-56A.

La chiave pubblica momentanea per l'accordo delle chiavi è archiviata insieme alla chiave per file protetta. KDF è la funzione di derivazione della chiave di concatenazione (alternativa 1 approvata) come descritto al punto 5.8.1 di NIST SP 800-56A. AlgorithmID è omesso. PartyUInfo e PartyVInfo sono chiavi pubbliche momentanee e statiche, rispettivamente. SHA-256 è usato come funzione di hashing. Non appena viene chiuso il file, la chiave per-file viene cancellata dalla memoria. Per potere aprire nuovamente il file, il segreto condiviso è ricreato utilizzando la chiave privata della classe "Protetto se non è aperto" e la chiave pubblica momentanea, che sono usate per aprire la chiave per-file utilizzata per decodificare il file.

Protetto fino alla prima autenticazione utente

(`NSFileProtectionCompleteUntilFirstUserAuthentication`): questa classe si comporta nello stesso modo di "Protezione completa", l'unica differenza è che la chiave di classe decodificata non viene rimossa dalla memoria quando il dispositivo è bloccato. La protezione in questa classe ha proprietà simili alla codifica desktop full-volume e protegge i dati dagli attacchi che prevedono un riavvio. Questa classe è quella di default per tutti i dati delle app di terze parti che non sono stati assegnati a una classe di protezione dati specifica.

Nessuna protezione

(`NSFileProtectionNone`): questa chiave di classe è protetta solo con l'UID ed è conservata in Effaceable Storage. Dato che tutte le chiavi necessarie per decodificare i file in questa classe sono archiviate sul dispositivo, la codifica può solo trarre vantaggio dalla cancellazione rapida a distanza. Se a un file non è stata assegnata una classe di protezione dati, è comunque archiviato in forma codificata (così come lo sono tutti i dati su un dispositivo iOS).

Chiave di classe per la protezione dei dati

Classe A	Protezione completa	(NSFileProtectionComplete)
Classe B	Protetto se non è aperto	(NSFileProtectionCompleteUnlessOpen)
Classe C	Protetto fino alla prima autenticazione utente	(NSFileProtectionCompleteUntilFirstUserAuthentication)
Classe D	Nessuna protezione	(NSFileProtectionNone)

Protezione dati del portachiavi

Molte app devono gestire password e altri dati non di grandi dimensioni ma sensibili, quali ad esempio chiavi e token di login. iOS fornisce un portachiavi sicuro in cui conservare questi elementi.

Gli elementi del portachiavi sono codificati tramite due diverse chiavi AES-256-GCM: una chiave per la tabella (metadati) e una chiave per ciascuna riga (chiave del valore segreto). I metadati del portachiavi (tutti gli attributi diversi da kSecValue) sono codificati con l'apposita chiave per velocizzare la ricerca, mentre i valori segreti (kSecValueData) vengono codificati con la chiave del valore segreto. La chiave dei metadati è protetta dal processore Secure Enclave, ma archiviata nella cache del processore per le applicazioni per consentire ricerche rapide del portachiavi. La chiave del valore segreto deve passare attraverso il processore di Secure Enclave.

Il portachiavi è implementato come un database SQLite archiviato nel file system. Esiste solo un database e il daemon *securityd* determina quali sono gli elementi del portachiavi a cui possono avere accesso i processi o le app. Le API di accesso al portachiavi eseguono chiamate al daemon, che a sua volta esegue la richiesta alle autorizzazioni "keychain-access-groups" "application-identifier" e "application-group" per l'app. I gruppi di accesso, piuttosto che limitare l'accesso a un singolo processo, consentono la condivisione tra app degli elementi del portachiavi.

Gli elementi del portachiavi possono essere condivisi solo tra app dello stesso sviluppatore. Perché sia possibile, viene richiesto alle app di terze parti di utilizzare gruppi di accesso con un prefisso assegnato a esse attraverso il programma per sviluppatori di iOS tramite i gruppi di applicazioni. La richiesta di prefisso e l'unicità di appartenenza a un gruppo di applicazioni sono applicate attraverso la firma del codice, i **profili di provisioning** e il programma per sviluppatori di Apple.

Componenti di un elemento del portachiavi

Insieme al gruppo di accesso, ogni elemento del portachiavi contiene i metadati amministrativi (per esempio le indicazioni temporali su creazione e ultimo aggiornamento).

Contiene anche gli hash SHA-1 degli attributi utilizzati per le richieste (come il nome di account e server) per consentire la ricerca senza decifrare ciascun elemento. Include infine i dati di codifica, che comprendono:

- Numero della versione.
- Dati sulla lista di controllo degli accessi (Access control list, ACL).
- Valore che indica la classe di protezione in cui è inserito l'elemento.
- Chiave per elemento cifrata con la chiave della classe di protezione.
- Dizionario degli attributi che descrivono l'elemento (come trasmessi a SecItemAdd), codificati come file plist binario, con la chiave per elemento.

La codifica è AES-256 in GCM (Galois/Counter Mode); il gruppo di accesso è compreso negli attributi e protetto dal tag GMAC calcolato durante la codifica.

I dati del portachiavi sono protetti utilizzando una struttura di classe simile a quella usata nella protezione dati dei file. Queste classi hanno comportamenti equivalenti alle classi di protezione dati dei file, ma usano chiavi distinte e fanno parte di API che hanno un nome diverso.

Disponibilità	Protezione dati dei file	Protezione dati del portachiavi
Quando sbloccato	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
Quando bloccato	NSFileProtectionCompleteUnlessOpen	N/A
Dopo primo sblocco	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Sempre	NSFileProtectionNone	kSecAttrAccessibleAlways
Codice abilitato	N/A	kSecAttrAccessible WhenPasscodeSetThisDeviceOnly

Le app che utilizzano servizi di aggiornamento in background possono usare `kSecAttrAccessibleAfterFirstUnlock` per quegli elementi del portachiavi a cui è necessario accedere durante gli aggiornamenti in background.

La classe `kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly` si comporta come `kSecAttrAccessibleWhenUnlocked`, tuttavia è disponibile solo quando il dispositivo è configurato con un codice. Questa classe esiste soltanto nella **keybag** di sistema. Queste classi:

- Non vengono sincronizzate sul portachiavi iCloud.
- Non vengono incluse nei backup.
- Non vengono incluse nelle keybag Escrow.

Se il codice viene rimosso o reimpostato, gli elementi vengono resi inutilizzabili eliminando le chiavi di classe.

Altre classi di portachiavi hanno una classe equivalente “Solo questo dispositivo”, sempre protetta con l'UID mentre viene copiata dal dispositivo durante un backup, per renderla inutilizzabile se ripristinata su un dispositivo diverso. Apple ha trovato l'equilibrio perfetto tra sicurezza e facilità d'uso scegliendo classi di portachiavi che dipendono dal tipo di informazione di cui si vuole garantire la sicurezza e da quando iOS la richiede. Ad esempio, un certificato VPN deve essere sempre disponibile affinché il dispositivo possa mantenere una connessione ininterrotta, ma è classificato come “non migratorio”, ovvero non può essere spostato su un altro dispositivo.

Per gli elementi del portachiavi creati da iOS, vengono applicate le protezioni di classe seguenti:

Elemento	Disponibile
Password Wi-Fi	Dopo primo sblocco
Account di posta	Dopo primo sblocco
Account Exchange	Dopo primo sblocco
Password VPN	Dopo primo sblocco
LDAP, CalDAV, CardDAV	Dopo primo sblocco
Token account social network	Dopo primo sblocco
Chiavi codifica annunci Handoff	Dopo primo sblocco
Token iCloud	Dopo primo sblocco
Password “In casa”	Quando sbloccato
Token “Trova il mio iPhone”	Sempre
Segreteria	Sempre
Backup iTunes	Quando sbloccato, non migratorio
Password Safari	Quando sbloccato
Segnalibri Safari	Quando sbloccato
Certificati VPN	Sempre, non migratorio
Chiavi Bluetooth®	Sempre, non migratorio
Token servizio notifiche push Apple	Sempre, non migratorio
Certificati iCloud e chiave privata	Sempre, non migratorio
Chiavi iMessage	Sempre, non migratorio
Certificati e chiavi private installate da un profilo di configurazione	Sempre, non migratorio
PIN SIM	Sempre, non migratorio

Controllo accesso portachiavi

I portachiavi possono usare delle ACL (access control lists) per impostare le politiche di accessibilità e i requisiti di autenticazione. Gli elementi possono stabilire delle condizioni che richiedono la presenza dell'utente specificando che non è possibile fornire l'accesso senza l'autenticazione tramite Touch ID, Face ID oppure inserendo il codice del dispositivo. L'accesso agli elementi può essere limitato specificando che la registrazione di Touch ID o Face ID non ha subito modifiche dal momento in cui l'elemento è stato aggiunto. Questa restrizione aiuta a impedire che un malintenzionato possa aggiungere la propria impronta digitale per accedere a un elemento del portachiavi. Gli elenchi ACL sono valutati all'interno di Secure Enclave e vengono rilasciati al kernel solo se si verificano i vincoli specificati.

Keybag

Le chiavi per le classi di protezione dati per i file e per il portachiavi sono raccolte e gestite in keybag. iOS utilizza le keybag seguenti: Utente, Dispositivo, Backup, Escrow e "Backup iCloud".

La **keybag Utente** è dove vengono archiviate le chiavi di classe cifrate usate durante il normale funzionamento del dispositivo. Ad esempio quando viene inserito un codice, la chiave `NSFileProtectionComplete` viene caricata dalla keybag Utente e viene decifrata. Si tratta di un file di elenco di proprietà binario (.plist) archiviato nella classe "Nessuna protezione", i cui contenuti sono codificati con una chiave contenuta in Effaceable Storage. Per poter fornire maggiore sicurezza alle keybag, questa chiave viene cancellata e rigenerata ogni volta che l'utente cambia il codice. L'estensione del kernel `AppleKeyStore` gestisce la keybag Utente e può essere interrogata sullo stato di blocco di un dispositivo. Riporterà che il dispositivo è sbloccato solo se tutte le chiavi di classe nella keybag Utente sono accessibili e sono state decifrate correttamente.

La **keybag Dispositivo** è utilizzata per l'archiviazione delle chiavi delle classi cifrate usate per operazioni che interessano dati specifici del dispositivo. A volte, i dispositivi iOS configurati per l'uso condiviso devono avere accesso alle credenziali prima che qualsiasi utente abbia effettuato il login; è quindi necessaria una keybag non protetta dal codice utente. iOS non supporta la separazione codificata del contenuto dei file system per utente: il sistema utilizzerà quindi le chiavi delle classi della keybag Dispositivo per la cifratura delle chiavi per file. Il portachiavi utilizza invece le chiavi delle classi della keybag Utente per proteggere gli elementi presenti nel portachiavi dell'utente. Sui dispositivi iOS configurati per essere utilizzati da un solo utente (configurazione di default), la keybag Dispositivo e quella Utente coincidono, protetta dal codice utente.

La **keybag Backup** è creata quando iTunes effettua un backup codificato e viene archiviata sul computer che contiene il backup del dispositivo. Viene creata una nuova keybag con un nuovo gruppo di chiavi e i dati di cui è stato eseguito il backup sono nuovamente codificati con queste chiavi nuove. Come è stato spiegato precedentemente, gli elementi del portachiavi non migratori rimangono cifrati con la chiave derivata dall'UID, consentendo così che possano venire ripristinati nel dispositivo da cui era stato eseguito il backup, ma rendendoli inaccessibili se spostati su un dispositivo diverso.

La keybag è protetta con la password impostata in iTunes, passata attraverso dieci milioni di iterazioni di PBKDF2. Nonostante questo alto numero di iterazioni, non è presente alcun legame a un dispositivo specifico e, per questo motivo, la keybag Backup potrebbe essere oggetto di un tentativo di attacco di forza bruta effettuato in parallelo su molti computer. È possibile ovviare a questa vulnerabilità utilizzando una password sufficientemente sicura.

Se un utente decide di non codificare un backup di iTunes, i file di backup non verranno codificati indipendentemente dalla classe di protezione dati a cui appartengono, ma il portachiavi rimane protetto con una chiave derivata dall'UID. Ecco perché gli elementi del portachiavi migrano su un nuovo dispositivo solo se è stata impostata una password di backup.

La **keybag Escrow** è utilizzata per la sincronizzazione con iTunes e per la gestione dei dispositivi mobili (MDM). Questa keybag consente a iTunes di eseguire il backup e la sincronizzazione senza richiedere all'utente di inserire un codice e permette a una soluzione MDM di cancellare remotamente il codice di un utente. È archiviata nel computer utilizzato per la sincronizzazione con iTunes o sulla soluzione MDM che gestisce il dispositivo da remoto.

La keybag Escrow migliora l'esperienza utente durante la sincronizzazione del dispositivo, operazione che potenzialmente potrebbe richiedere l'accesso a qualsiasi classe di dati. Quando un dispositivo bloccato da codice è connesso a iTunes per la prima volta, all'utente viene chiesto di inserire un codice. Il dispositivo crea quindi una keybag Escrow contenente le stesse chiavi di classe utilizzate sul dispositivo, protette da una chiave generata ex novo. La keybag Escrow e la chiave che la protegge sono divisi tra il dispositivo e l'host o il server, e i dati sono archiviati sul dispositivo nella classe “Protetto fino alla prima autenticazione utente”. Questo è il motivo per cui è necessario inserire il codice prima che l'utente esegua un backup con iTunes per la prima volta dopo un riavvio.

Nel caso di un aggiornamento software in modalità wireless, all'utente viene richiesto di inserire il codice all'avvio dell'aggiornamento. Questa procedura viene utilizzata per creare un token di sblocco, utilizzabile una sola volta, che sblocca la keybag Utente dopo l'aggiornamento. Il token non può essere generato senza inserire il codice dell'utente e qualsiasi token generato in precedenza viene invalidato se il codice dell'utente è stato modificato.

I token di sblocco utilizzabili una sola volta possono essere utilizzati per l'installazione assistita oppure non assistita di un aggiornamento software. Vengono codificati con una chiave derivata dal valore attuale di un contatore monotonico in Secure Enclave, l'UUID della keybag e l'UID di Secure Enclave.

Se il contatore del token di sblocco utilizzabile una sola volta viene incrementato in Secure Enclave, qualsiasi token esistente viene invalidato. Il contatore viene incrementato quando un token viene utilizzato, dopo il primo sblocco di un dispositivo riavviato, quando un aggiornamento software viene annullato (dall'utente o dal sistema) o quando il timer per la validità del token è scaduto.

Il token di sblocco utilizzabile una sola volta per gli aggiornamenti software assistiti scade dopo 20 minuti. Il token viene esportato da Secure Enclave e viene scritto in Effaceable Storage. Se il dispositivo non viene riavviato entro 20 minuti, il timer per la validità fa incrementare il contatore.

Gli aggiornamenti software automatici avvengono quando il sistema rileva che è disponibile un aggiornamento e:

- Gli aggiornamenti automatici sono configurati su iOS 12.

  Oppure

- L'utente sceglie “Installa più tardi” quando riceve una notifica dell'aggiornamento.

Una volta che l'utente ha inserito il codice, viene generato un token di sblocco una tantum che può restare valido in Secure Enclave per 8 ore. Se l'aggiornamento non si è ancora verificato, questo token di sblocco viene distrutto a ciascun blocco e ricreato a ciascuno sblocco successivo. Ciascuno sblocco riavvia la finestra di 8 ore.

Dopo 8 ore, un timer renderà il token di sblocco non valido.

La **keybag "Backup iCloud"** è simile alla keybag Backup. Tutte le chiavi di classe in questa keybag sono asimmetriche (utilizzano Curve25519, come la classe di protezione dati "Protetto se non è aperto"), di conseguenza i backup di iCloud possono venire eseguiti in background. Per tutte le classi di protezione dati, fatta eccezione per "Nessuna protezione", i dati codificati sono letti dal dispositivo e inviati a iCloud. Le chiavi di classe corrispondenti sono protette dalle chiavi di iCloud. Le chiavi di classe del portachiavi sono cifrate con una chiave derivata dall'UID proprio come nel caso di un backup di iTunes non codificato. Per il backup nella funzione di recupero del portachiavi iCloud viene utilizzata anche una keybag asimmetrica.

Sicurezza delle app

Le app sono senza dubbio degli elementi cruciali all'interno di un'architettura mobile moderna e sicura. Se da un lato le app apportano agli utenti incredibili benefici dal punto di vista della produttività, dall'altro rappresentano un rischio potenziale per la sicurezza del sistema, la stabilità e i dati dell'utente se non sono gestite correttamente.

Per questo motivo, iOS fornisce vari livelli di protezione per garantire che le app siano firmate e verificate, e che siano "sandboxed" (ossia non possono accedere ai dati archiviati da altre applicazioni) per proteggere i dati dell'utente. Questi elementi forniscono alle app una piattaforma stabile e sicura, permettendo a migliaia di sviluppatori di distribuire centinaia di migliaia di app su iOS senza compromettere l'integrità del sistema. Inoltre gli utenti possono accedere a tali app sui dispositivi iOS senza temere virus, malware o attacchi non autorizzati.

Firma del codice delle app

Il kernel di iOS, una volta avviato, controlla i processi utente e le app che possono venire eseguite. Per assicurarsi che tutte le app provengano da una fonte conosciuta e approvata, e che non siano state danneggiate, iOS richiede che tutto il codice eseguibile venga firmato utilizzando un certificato emesso da Apple. Le app fornite con il dispositivo, come Mail e Safari, sono firmate da Apple. Anche le app di terze parti devono essere convalidate e firmate utilizzando un certificato emesso da Apple. La firma del codice obbligatoria estende il concetto di catena di fiducia e lo porta dal sistema operativo alle app, e impedisce alle app di terze parti di caricare risorse codice non firmate o di usare codice auto modificante.

Per poter sviluppare e installare app sui dispositivi iOS, gli sviluppatori devono registrarsi presso Apple e prendere parte al programma per sviluppatori di Apple. Prima di emettere il certificato, Apple verifica l'identità reale di ogni sviluppatore, sia esso un individuo o un'azienda. Questo certificato abilita gli sviluppatori a firmare le app e a inviarle a App Store per la distribuzione. Il risultato è dunque che tutte le app presenti in App Store sono state consegnate da una persona o da un'organizzazione identificabile, e serve come deterrente per la creazione di app pericolose. Inoltre, sono state verificate da Apple per garantire che operino come descritto e che non contengano errori evidenti o altri problemi. Oltre alla tecnologia di cui abbiamo parlato poco fa, questo processo di cura dei dati crea nei clienti un sentimento di fiducia nei confronti delle app da loro acquistate.

iOS permette agli sviluppatori di incorporare nelle proprie app dei framework che possono essere utilizzati dall'app stessa o da estensioni incorporate all'interno dell'app. Per proteggere il sistema e altre app ed evitare che carichino codice di terze parti all'interno del loro spazio di indirizzi, il sistema eseguirà una convalida della firma del codice di tutte le librerie dinamiche a cui un processo si collega all'avvio. Questa verifica si compie attraverso l'identificatore di team (Team ID), che viene estratto da un certificato emesso da Apple. Un identificatore di team è una stringa alfanumerica di lunghezza pari a 10 caratteri; ad esempio, 1A2B3C4D5F.

Un programma può collegarsi a ogni libreria di piattaforma fornita con il sistema, oppure ogni libreria con lo stesso identificatore di team nella firma di codice come eseguibile principale. Dal momento che gli eseguibili forniti come parte del sistema non hanno un identificatore di team, potranno solo collegarsi a librerie facenti parte del sistema stesso.

Le aziende hanno anche la capacità di scrivere app in-house da utilizzare all'interno dell'organizzazione e da distribuire ai propri dipendenti. Le aziende e le organizzazioni possono iscriversi al programma ADEP (Apple Developer Enterprise Program) con un numero D-U-N-S. Apple dà l'approvazione solo dopo aver verificato l'identità e l'idoneità dei richiedenti. Una volta che un'organizzazione diventa un membro dell'ADEP, può registrarsi per ottenere un profilo di provisioning che permetta alle app in-house di essere eseguite sui dispositivi autorizzati. Gli utenti devono a loro volta avere il profilo di provisioning installato per poter eseguire le app in-house. In questo modo si garantisce che solo gli utenti previsti dall'organizzazione siano in grado di caricare le app sui propri dispositivi iOS. Le app installate via MDM sono considerate implicitamente affidabili, perché la relazione tra l'organizzazione e il dispositivo è già stata stabilita. Negli altri casi, gli utenti devono approvare il profilo di provisioning dell'app in Impostazioni. Le organizzazioni possono impedire agli utenti di approvare app provenienti da sviluppatori sconosciuti. Al primo avvio di qualsiasi app aziendale, il dispositivo deve ricevere da Apple una conferma positiva del consenso a eseguire l'app.

A differenza di altre piattaforme mobili, iOS non consente agli utenti di installare app non firmate potenzialmente nocive scaricate da siti web, e nemmeno di eseguire codice non attendibile. Durante l'esecuzione, le verifiche delle firme del codice di tutte le pagine di memoria eseguibili sono realizzate mentre vengono caricate, per garantire che un'app non sia stata modificata dall'ultima volta che è stata installata o aggiornata.

Sicurezza del processo di runtime

Una volta verificato che l'app proviene da una fonte approvata, iOS mette in pratica le misure di sicurezza progettate evitare che altre app o il resto del sistema vengano compromessi.

Tutte le app di terze parti sono “sandboxed”, ovvero non possono accedere ai file archiviati da altre applicazioni o apportare delle modifiche al dispositivo. Questo meccanismo fa sì che le app non possano raccogliere o modificare le informazioni archiviate da altre app. Ogni app dispone di una directory home unica per i propri file, che viene assegnata in maniera casuale al momento dell'installazione della app. Se un'app di terze parti deve accedere a informazioni diverse dalle proprie, lo può fare unicamente usando i servizi forniti specificamente da iOS.

Anche i file di sistema e le risorse vengono protetti dalle app dell'utente. La maggior parte di iOS viene eseguita come piattaforma utente mobile non privilegiata, come succede per tutte le app di terze parti. L'intera partizione del sistema operativo è montata come volume di sola lettura. Gli strumenti non necessari, come i servizi di login remoto, non sono inclusi nel software di sistema e le API non consentono alle app di far valere i propri privilegi per modificare altre app o iOS stesso.

L'accesso a funzionalità e informazioni dell'utente, come ad esempio iCloud ed estensibilità, da parte di app di terze parti è controllato utilizzando autorizzazioni dichiarate. Le autorizzazioni sono coppie di valori chiave registrate in un'app e che consentono l'autenticazione

indipendentemente da altri fattori di runtime, come l'ID utente Unix. Dato che le autorizzazioni sono firmate digitalmente, non possono essere modificate. Le autorizzazioni sono ampiamente usate da app di sistema e daemon per eseguire operazioni privilegiate specifiche che richiederebbero altrimenti di eseguire il processo come root. In questo modo si riduce al minimo il rischio potenziale di sorpasso dei privilegi da parte di un'app di sistema o daemon compromessi.

Inoltre, le app possono solo eseguire processi in background tramite API fornite dal sistema. Ciò consente alle app di continuare a funzionare senza peggiorare le prestazioni o senza avere un impatto significativo sulla durata della batteria.

ASLR (Address space layout randomization) è un meccanismo che serve a proteggere il sistema contro lo sfruttamento di bug che causano danneggiamento della memoria. Le app incorporate usano ASLR per assicurare che tutte le regioni della memoria vengano assegnate in modo casuale all'avvio. La distribuzione casuale degli indirizzi di memoria del codice eseguibile, delle librerie di sistema e dei blocchi di programmazione relativi riduce la probabilità di molti attacchi sofisticati. Ne sono un esempio i tentativi di attacco return-to-libc mirati a ingannare il dispositivo affinché esegua codice maligno manipolando gli indirizzi di memoria delle librerie dello stack e del sistema. La posizione casuale degli indirizzi di memoria rende molto più difficile eseguire l'attacco, specialmente su diversi dispositivi. Xcode, l'ambiente di sviluppo iOS, aderisce automaticamente ai programmi di terze parti con il supporto ASLR attivato.

iOS fornisce un ulteriore strumento di protezione utilizzando la funzionalità Execute Never (XN) di ARM, che contrassegna le pagine di memoria come non eseguibili. Le pagine di memoria contrassegnate come scrivibili ed eseguibili possono essere utilizzate solo da app sotto condizioni estremamente controllate. Il kernel verifica la presenza dell'autorizzazione per la firma del codice dinamico esclusiva di Apple. Dopo ciò, può comunque essere effettuata solo una singola chiamata mmap per richiedere una pagina scrivibile ed eseguibile, a cui viene assegnato un indirizzo casuale. Safari utilizza questa funzionalità per il compilatore JIT JavaScript.

Estensioni

iOS consente alle app di fornire funzionalità ad altre app attraverso le *estensioni*. Le estensioni sono binari eseguibili firmati con uno scopo specifico, inseriti in un pacchetto all'interno di un'app. Il sistema le rileva automaticamente al momento dell'installazione e le rende disponibili per le altre app che utilizzano un sistema corrispondente.

L'area di sistema che supporta le estensioni è chiamata *punto di estensione*. Ogni punto di estensione fornisce delle API e applica delle politiche per quell'area specifica. Il sistema determina le estensioni disponibili basandosi su regole di corrispondenza specifiche per ciascun punto di estensione. Il sistema avvia automaticamente i processi di estensione quando necessario e ne gestisce la durata. Per limitare la disponibilità delle estensioni ad app di sistema specifiche, possono essere utilizzate le autorizzazioni. Ad esempio, un widget per la schermata Oggi compare solo in Centro Notifiche e un'estensione di condivisione è disponibile solo dal pannello Condivisione. I punti di estensione sono i widget della schermata Oggi, la condivisione, le azioni personalizzate, la modifica delle foto, i provider di documenti e le tastiere personalizzate.

Le estensioni vengono eseguite nel proprio spazio di indirizzo. La comunicazione tra l'estensione e l'app che l'ha attivata utilizza comunicazioni inter-process (IPC) mediate dal framework di sistema. Non hanno accesso ai rispettivi file o spazi di memoria. Le estensioni sono progettate per essere isolate l'una dall'altra, oltre che dalle app che le contengono e da quelle che le utilizzano. Sono "sandboxed" come ogni altra app di terze parti e dispongono di un contenitore separato da quello che contiene l'app. Condividono comunque lo stesso accesso ai controlli per la privacy. Quindi se un utente concede a un'app l'accesso a Contatti, questa concessione verrà estesa alle estensioni che sono incorporate all'interno dell'app, ma non a quelle attivate dall'app.

Le tastiere personalizzate sono un tipo speciale di estensione, poiché vengono abilitate dall'utente per l'intero sistema. Una volta abilitata, viene utilizzata un'estensione tastiera per qualsiasi campo di testo, fatta eccezione per quello di inserimento del codice e altri campi riservati alla visualizzazione di testo sicuro. Per limitare il trasferimento dei dati dell'utente, le tastiere personalizzate vengono eseguite di default in una sandbox molto restrittiva che blocca l'accesso alla rete, ai servizi che eseguono operazioni di rete per conto di un processo e ad API che permetterebbero all'estensione di far trapelare dati di digitazione. Gli sviluppatori di tastiere personalizzate possono richiedere che le loro estensioni abbiano Open Access, che permetterà al sistema di eseguire l'estensione nella sandbox di default dopo aver ottenuto il consenso dell'utente.

Per i dispositivi registrati in una soluzione MDM, le estensioni di documenti e tastiere rispettano le regole Managed Open In. Ad esempio, la soluzione MDM può impedire che un utente esporti un documento da un'app gestita a un provider di documenti non gestito, oppure utilizzi una tastiera non gestita con un'app gestita. Inoltre, gli sviluppatori di app possono impedire l'uso di estensioni di tastiera di terze parti all'interno della propria app.

Gruppi di app

Le app e le estensioni possedute da un determinato account sviluppatore possono condividere i contenuti se configurate per fare parte di un gruppo di app. È compito dello sviluppatore creare i gruppi appropriati sul portale Apple Developer Portal e includere l'insieme desiderato di app ed estensioni. Le app, dopo essere state configurate come parte di un gruppo di app, hanno accesso a:

- Un contenitore sul volume condiviso per l'archiviazione che rimane sul dispositivo fino a quando almeno una delle app appartenenti al gruppo è installata.
- Preferenze condivise.
- Elementi del portachiavi condivisi.

Il portale Apple Developer Portal garantisce che gli ID dei gruppi di app siano unici in tutto l'ecosistema di app.

Protezione dati nelle app

Il kit SDK (Software Development Kit) di iOS offre una suite completa di API grazie alla quale gli sviluppatori di terze parti e in-house possono adottare con estrema facilità la protezione dati e che garantisce il massimo livello di protezione nelle app. La protezione dati è disponibile per API di file e di database, inclusi NSFileManager, CoreData, NSData e SQLite.

Il database dell'app Mail (inclusi gli allegati), i libri gestiti, i segnalibri di Safari, le immagini all'avvio delle app e i dati di localizzazione sono archiviati tramite codifica con chiavi protette mediante il codice dell'utente sul dispositivo. Calendario (esclusi gli allegati), Contatti, Promemoria, Note, Messaggi e Foto implementano la protezione dati "Protetto fino alla prima autenticazione utente".

Le app installate dall'utente che non optano per una classe specifica di protezione dati ricevono automaticamente la classe "Protetto fino alla prima autenticazione utente".

Accessori

Il programma di licenze MFi (Made for iPhone, iPad, and iPod touch) fornisce ai produttori di accessori verificati l'accesso al protocollo iAP (iPod Accessories Protocol) oltre che ai componenti di supporto hardware necessari.

Quando un accessorio MFi comunica con un dispositivo iOS utilizzando un connettore Lightning o attraverso Bluetooth, il dispositivo chiede all'accessorio di dimostrare che è stato autorizzato da Apple rispondendo con un certificato fornito da Apple stessa, che viene verificato dal dispositivo. Il dispositivo invia successivamente una richiesta a cui l'accessorio deve rispondere con una risposta firmata. Questo processo è interamente gestito da un circuito integrato personalizzato che Apple fornisce ai produttori di accessori approvati e che è trasparente all'accessorio stesso.

Gli accessori possono richiedere l'accesso a metodi di trasporto e funzionalità diversi, come ad esempio l'accesso a stream audio digitali via cavo Lightning oppure le informazioni di localizzazione fornite tramite Bluetooth. Un circuito integrato di autenticazione garantisce che il pieno accesso al dispositivo venga concesso solo agli accessori approvati. Se un accessorio non supporta l'autenticazione, il suo accesso verrà limitato all'audio analogico e a un numero limitato di controlli di riproduzione audio seriali (UART).

Anche AirPlay utilizza l'autenticazione con circuito integrato per verificare che i ricevitori siano stati approvati da Apple. Gli stream audio AirPlay e video CarPlay utilizzano il protocollo MFi-SAP (Secure Association Protocol), che codifica la comunicazione tra l'accessorio e il dispositivo utilizzando AES-128 in modalità CTR. Le chiavi effimere sono scambiate usando lo scambio di chiavi ECDH (Curve25519) e firmate utilizzando la chiave RSA a 1024 bit del circuito integrato di autenticazione come parte del protocollo STS (station-to-station).

HomeKit

HomeKit fornisce un'infrastruttura di automazione domestica che utilizza la sicurezza di iCloud e iOS per proteggere e sincronizzare i dati privati senza esporli ad Apple.

Identità HomeKit

L'identità e la sicurezza di HomeKit sono basate su coppie di chiavi pubbliche-private Ed25519. Sul dispositivo iOS viene generata una coppia di chiavi Ed25519 per ogni utente di HomeKit, e questa diventa la sua identità HomeKit. Questa è usata per autenticare la comunicazione tra i dispositivi iOS, e tra i dispositivi iOS e gli accessori.

Le chiavi vengono archiviate in Portachiavi e sono incluse solo in backup codificati di Portachiavi. Le chiavi sono sincronizzate tra i dispositivi utilizzando il portachiavi iCloud, dove disponibile. HomePod e Apple TV ricevono le chiavi mediante la configurazione tramite tocco o la modalità di configurazione descritte di seguito. Le chiavi sono condivise da iPhone a un Apple Watch abbinato tramite il servizio di identificazione Apple.

Comunicazione con gli accessori HomeKit

Gli accessori HomeKit generano la loro coppia di chiavi Ed25519 da utilizzare nelle comunicazioni con i dispositivi iOS. Se l'accessorio è ripristinato alle impostazioni di fabbrica, viene generata una nuova coppia.

Per stabilire una relazione tra un dispositivo iOS e un accessorio HomeKit, le chiavi vengono scambiate utilizzando il protocollo Secure Remote Password (a 3072 bit), usando un codice a otto cifre fornito dal produttore dell'accessorio e inserito sul dispositivo iOS dall'utente e successivamente codificato mediante CHACHA20-POLY1305 AEAD con chiavi derivate da HKDF-SHA-512. Durante la configurazione viene verificata anche la certificazione MFi dell'accessorio. Gli accessori senza un chip MFi possono integrare il supporto per l'autenticazione software su iOS 11.3 o versione successiva.

Quando il dispositivo iOS e l'accessorio HomeKit comunicano durante l'utilizzo, il primo autentica il secondo, e viceversa, utilizzando le chiavi scambiate nel processo descritto qui sopra. Ogni sessione è stabilita utilizzando il protocollo Station-to-Station ed è codificata con chiavi derivate da HKDF-SHA-512 basate su chiavi Curve25519 per sessione. Questo è valido sia per accessori basati su IP sia su quelli Bluetooth Low Energy.

Per i dispositivi Bluetooth Low Energy che supportano le notifiche broadcast, all'accessorio viene fornita una chiave di codifica broadcast da un dispositivo iOS abbinato tramite una sessione sicura. Tale chiave è utilizzata per codificare i dati riguardo alle modifiche di stato sull'accessorio, che vengono comunicate tramite trasmissioni Bluetooth Low Energy. La chiave di codifica broadcast è una chiave derivata tramite HKDF-SHA-512 e i dati sono codificati con l'algoritmo CHACHA20-POLY1305 AEAD (Authenticated Encryption with Associated Data). La chiave di codifica broadcast viene modificata periodicamente dal dispositivo iOS e sincronizzata su altri dispositivi che utilizzano iCloud, come descritto nella sezione “Sincronizzazione dati tra dispositivi e utenti” più avanti.

Archiviazione dei dati locali

HomeKit archivia sul dispositivo iOS dell'utente i dati relativi ad abitazione, accessori, luoghi e utenti. Questi dati archiviati sono codificati utilizzando le chiavi derivate dalle chiavi di identità HomeKit dell'utente, oltre a un nonce casuale. Inoltre, i dati HomeKit sono archiviati utilizzando la classe di protezione dati "Protetto fino alla prima autenticazione utente". I dati HomeKit sono inclusi solo in backup codificati, così, ad esempio, i backup di iTunes non codificati non conterranno i dati HomeKit.

Sincronizzazione dati tra dispositivi e utenti

I dati di HomeKit possono essere sincronizzati tra i dispositivi iOS di un utente utilizzando iCloud e il portachiavi iCloud. I dati HomeKit sono codificati durante la sincronizzazione utilizzando chiavi derivate dall'identità HomeKit dell'utente e dal nonce casuale. Durante la sincronizzazione, tali dati vengono gestiti come un blob opaco. Il blob più recente è archiviato su iCloud per abilitare la sincronizzazione, ma non è utilizzato per altri scopi. È un oggetto codificato utilizzando chiavi disponibili solo sui dispositivi iOS dell'utente e quindi il suo contenuto è inaccessibile durante la trasmissione e l'archiviazione iCloud.

I dati HomeKit sono anche sincronizzati tra utenti multipli della stessa abitazione. Questo processo utilizza autenticazione e codifica, proprio come quelle usate tra un dispositivo iOS e un accessorio HomeKit. L'autenticazione è basata su chiavi pubbliche Ed25519 che vengono scambiate tra i dispositivi quando un utente viene aggiunto a un'abitazione Dopo che un nuovo utente è stato aggiunto a un'abitazione, ogni comunicazione successiva è autenticata e codificata utilizzando il protocollo Station-to-Station e le chiavi specifiche per sessione.

I nuovi utenti possono essere aggiunti dall'utente che ha inizialmente creato l'abitazione in HomeKit o da un altro utente con permessi di modifica. Il dispositivo del proprietario configura gli accessori con la chiave pubblica del nuovo utente affinché l'accessorio possa autenticarsi e accettare comandi dall'utente nuovo. Quando un utente che dispone di permessi di modifica aggiunge un nuovo utente, il processo viene delegato a un hub domestico per completare l'operazione.

Il processo destinato ad abilitare l'uso di Apple TV con HomeKit viene realizzato automaticamente quando l'utente effettua l'accesso a iCloud. L'account di iCloud richiede che sia abilitata l'autenticazione a due fattori. Apple TV e il dispositivo del proprietario si scambiano momentaneamente le chiavi pubbliche Ed25519 via iCloud. Quando il dispositivo del proprietario e Apple TV si trovano sulla stessa rete locale, le chiavi temporanee vengono utilizzate per proteggere una connessione sulla rete locale tramite il protocollo Station-to-Station e le chiavi per sessione. Questo processo utilizza autenticazione e codifica, proprio come quelle usate tra un dispositivo iOS e un accessorio HomeKit. Tramite questa connessione locale protetta, il dispositivo del proprietario trasferisce le coppie di chiavi pubbliche-private Ed25519 dell'utente ad Apple TV. Queste chiavi vengono quindi utilizzate per proteggere la comunicazione tra Apple TV e gli accessori HomeKit così come tra Apple TV e altri dispositivi iOS appartenenti all'abitazione di HomeKit.

Se un utente non dispone di vari dispositivi e non concede l'accesso alla propria abitazione ad altri utenti, non verrà sincronizzato con iCloud nessun dato di HomeKit.

Dati abitazione e app

L'accesso ai dati dell'abitazione da parte delle app è controllato dalle impostazioni sulla privacy dell'utente. Agli utenti viene chiesto di concedere l'accesso quando le app richiedono dati dell'abitazione, come avviene per Contatti, Foto e altre sorgenti di dati iOS. Se l'utente dà la propria autorizzazione, le app avranno accesso ai nomi delle stanze, ai nomi degli accessori e alle informazioni di ubicazione degli accessori nelle stanze, oltre ad altri dati, come spiegato in dettaglio nella documentazione HomeKit per gli sviluppatori, disponibile su: https://developer.apple.com/homekit/.

HomeKit e Siri

Siri può essere utilizzato per inviare richieste agli accessori, controllarli e per attivare le scene. Siri riceve le informazioni essenziali sulla configurazione dell'abitazione, in modo da fornire i nomi di stanze, accessori e scene necessari al riconoscimento dei comandi. L'audio inviato a Siri potrebbe indicare dei comandi o degli accessori specifici, ma tali dati di Siri non sono associati ad altre funzionalità di Apple come HomeKit. Per ulteriori informazioni, consulta "Siri", nella sezione di questo documento dedicata ai servizi Internet.

Videocamere IP per HomeKit

Le videocamere IP in HomeKit inviano stream video e audio direttamente al dispositivo iOS sulla rete locale che ha accesso allo stream. Gli stream sono codificati tramite chiavi generate casualmente sul dispositivo iOS e sulla videocamera IP, che sono scambiate tramite la sessione HomeKit protetta con la videocamera. Quando il dispositivo iOS non si trova sulla rete locale, gli stream codificati sono trasmessi attraverso l'hub domestico verso il dispositivo iOS. L'hub domestico non decodifica gli stream e funge solo da elemento di trasmissione tra il dispositivo iOS e la videocamera IP. Quando un'app mostra il video della videocamera IP di HomeKit all'utente, HomeKit elabora i fotogrammi in maniera protetta da un processo di sistema separato, in modo tale che l'app non sia in grado di accedere allo stream video o di archiviarlo. Inoltre, alle app non è consentito eseguire istantanee schermo dello stream.

Accesso remoto via iCloud per gli accessori HomeKit

Gli accessori HomeKit possono connettersi direttamente a iCloud per consentire ai dispositivi iOS di controllarli quando la comunicazione Bluetooth o Wi-Fi non è disponibile.

L'accesso remoto via iCloud è stato progettato in maniera tale che ogni accessorio possa essere controllato e possa inviare notifiche senza rivelare ad Apple di che accessorio si tratti o quali comandi o notifiche sta inviando. HomeKit non invia informazioni sull'abitazione tramite l'accesso remoto via iCloud.

Quando un utente invia un comando tramite l'accesso remoto via iCloud, viene stabilita un'autenticazione reciproca tra l'accessorio e il dispositivo iOS e i dati vengono codificati tramite la stessa procedura descritta per le connessioni locali. I contenuti delle comunicazioni sono codificati e non sono visibili da parte di Apple. Il collegamento tramite iCloud è basato sugli identificatori di iCloud registrati durante il processo di configurazione.

Gli accessori che supportano l'accesso remoto via iCloud vengono abbinati durante il loro processo di configurazione. Il processo di abbinamento inizia quando l'utente effettua l'accesso a iCloud. Successivamente il dispositivo iOS chiede all'accessorio di autenticarsi tramite l'apposito coprocessore Apple integrato in tutti gli accessori compatibili con HomeKit. L'accessorio genera anche chiavi basate su curve ellittiche prime256v1 e la chiave pubblica viene inviata al dispositivo iOS insieme all'autenticazione e al certificato X.509 del coprocessore per l'autenticazione. Essi vengono utilizzati per richiedere un certificato per l'accessorio dal server di provisioning di iCloud. Il certificato viene archiviato dall'accessorio, ma non contiene nessuna informazione che lo identifichi, a parte il permesso di connettersi tramite l'accesso remoto via iCloud di HomeKit. Il dispositivo iOS che sta eseguendo il provisioning invia all'accessorio anche l'URL e altre informazioni necessarie a connettersi al server di accesso remoto di iCloud. Tali informazioni non sono legate a nessun utente o accessorio.

Ogni accessorio registra un elenco di utenti consentiti per il server di accesso remoto di iCloud. Tali utenti hanno ricevuto il permesso di controllare l'accessorio dalla persona che lo ha aggiunto all'abitazione. Agli utenti viene assegnato un identificatore dal server di iCloud e possono essere associati a un account iCloud allo scopo di consegnare messaggi di notifica e risposte da parte degli accessori. Analogamente, gli accessori ricevono degli identificatori da iCloud, ma tali identificatori non rivelano alcuna informazione sull'accessorio stesso.

Quando un accessorio si connette al server di accesso remoto via iCloud di HomeKit, presenta il proprio certificato e un permesso. Il permesso viene ottenuto da un altro server iCloud e non è unico per ogni accessorio. Quando un accessorio richiede un permesso, nella richiesta vengono inclusi il produttore, il modello e la versione del firmware. Con la richiesta non viene inviata alcuna informazione che identifichi l'utente o l'abitazione. La connessione al server che fornisce i permessi non è autenticata, in maniera tale da proteggere maggiormente la privacy.

Gli accessori si connettono al server di accesso remoto via iCloud attraverso HTTP/2, protetto tramite TLS 1.2 con AES-128-GCM e SHA-256. L'accessorio mantiene aperta la connessione al server di accesso remoto via iCloud, in maniera tale da poter ricevere messaggi e inviare risposte e notifiche ai dispositivi iOS.

Telecomandi TV HomeKit

I telecomandi TV di terze parti compatibili con HomeKit forniscono eventi HID e audio Siri a un'Apple TV associata aggiunta tramite l'app Casa. Gli eventi HID vengono inviati attraverso la sessione sicura tra Apple TV e il telecomando. Un telecomando TV compatibile con Siri invia dati audio a Apple TV quando l'utente attiva esplicitamente il microfono sul telecomando tramite un tasto dedicato a Siri. I fotogrammi audio vengono inviati direttamente a Apple TV tramite una connessione di rete locale dedicata tra Apple TV e il telecomando. La connessione di rete locale è codificata con una coppia di chiavi derivate tramite HKDF-SHA-512 che è negoziata attraverso la sessione HomeKit tra Apple TV e il telecomando TV. HomeKit decodifica i fotogrammi audio su Apple TV e li inoltra all'app Siri, dove vengono trattati con le stesse protezioni della privacy applicate a tutti gli input audio di Siri.

SiriKit

Siri utilizza il meccanismo delle estensioni iOS per comunicare con le app di terze parti. Nonostante abbia accesso ai contatti di iOS e alla posizione attuale del dispositivo, prima di fornire tali informazioni all'app, Siri verifica che l'app che contiene l'estensione abbia il permesso di accedere ai dati utente protetti da iOS. Siri passa all'estensione solo il frammento rilevante della richiesta originale dell'utente. Ad esempio, se l'app non ha accesso ai contatti di iOS, Siri non risolverà la relazione contenuta in una richiesta dell'utente del tipo "Invia 10 € a mia madre con (app di pagamento)". In questo caso, l'app dell'estensione riconoscerebbe solo "madre" nel frammento di richiesta che le viene passato. Tuttavia, se l'app ha accesso ai contatti di iOS, riceve le informazioni relative alla madre dell'utente dai contatti di iOS. Se un contatto viene menzionato nel corpo di un messaggio, come ad esempio "Invia un messaggio a mamma su (app di messaggistica) e dille che mio fratello è stato bravissimo", Siri non elaborerà "mio fratello" a prescindere dai TCC dell'app. I contenuti presentati dall'app potrebbero essere inviati al server per consentire a Siri di comprendere il vocabolario che l'utente potrebbe utilizzare nell'app. In casi come "Trovami un'auto per andare a casa di mia madre utilizzando (nome app)", in cui la richiesta dell'utente necessita la ricezione delle informazioni sulla posizione dai contatti dell'utente, Siri fornisce tali informazioni all'estensione dell'app, solo per tale richiesta, a prescindere dalla posizione dell'app o dall'accesso ai contatti.

In fase di esecuzione, Siri consente all'app compatibile con SiriKit di fornire un insieme di parole personalizzate specifiche per l'istanza dell'app. Queste parole personalizzate sono legate all'identificatore casuale discusso nella sezione dedicata a Siri di questo documento e hanno la stessa durata.

HealthKit

HealthKit archivia e aggiunge i dati delle app di salute e fitness con il consenso dell'utente. Funziona anche direttamente con i dispositivi per salute e fitness, come i cardiofrequenzimetri compatibili con Bluetooth Low Energy (BLE) e i coprocessori di movimento integrati in molti dispositivi iOS.

Dati sanitari

HealthKit consente agli utenti di archiviare e aggregare i propri dati sanitari da fonti come app, dispositivi e istituti sanitari. Tali dati sono archiviati nella classe di protezione dati "Protetto se non è aperto". L'accesso ai dati viene revocato 10 minuti dopo il blocco del dispositivo e i dati tornano accessibili la volta successiva che l'utente inserisce il codice o utilizza Touch ID o Face ID per sbloccare il dispositivo.

HealthKit aggiunge inoltre dei dati di gestione, come i permessi di accesso per le app, i nomi dei dispositivi connessi a HealthKit e le informazioni sulla programmazione utilizzate per aprire le app quando sono disponibili nuovi dati. Tali dati sono archiviati nella classe di protezione dati "Protetto fino alla prima autenticazione utente".

I file journal temporanei archiviano le informazioni sanitarie generate quando il dispositivo è bloccato, ad esempio quando l'utente sta facendo esercizio fisico. Tali informazioni sono archiviate nella classe di protezione dati "Protetto se non è aperto". Quando il dispositivo è sbloccato, i file journal temporanei vengono importati nel database sanitario di base e successivamente eliminati una volta completato il processo.

I dati sanitari possono essere archiviati su iCloud. Quando sono configurati per l'archiviazione su iCloud, i dati sanitari vengono sincronizzati tra i dispositivi e resi sicuri tramite una codifica che li protegge sia mentre sono in transito che quando sono archiviati. I dati sanitari vengono inclusi solo nei backup di iTunes codificati. Non vengono inclusi in backup di iTunes o di iCloud non codificati.

Dati sanitari clinici

Gli utenti possono accedere a sistemi sanitari supportati all'interno dell'app Salute per ottenere una copia dei propri dati sanitari clinici. Durante la connessione a un sistema sanitario, l'utente effettua l'autenticazione tramite credenziali client OAuth 2. Dopo la connessione, i dati sanitari clinici vengono scaricati direttamente dall'istituto sanitario tramite una connessione protetta TLS v1.2. Una volta scaricati, tali dati vengono archiviati in maniera sicura assieme ai dati sanitari.

Integrità dei dati

I dati archiviati nel database includono metadati per rintracciare la provenienza di ogni record di dati. Questi metadati includono a loro volta un identificatore per l'app che identifica l'applicazione che ha archiviato il record. In aggiunta a questo, un elemento di metadati opzionale può contenere una copia digitalmente firmata del record. Questo accorgimento ha lo scopo di garantire l'integrità di dati per i record generati da un dispositivo attendibile. Il formato utilizzato per la firma digitale è CMS (Cryptographic Message Syntax), specificato in IETF RFC 5652.

Accesso da parte di app di terze parti

L'accesso all'API di HealthKit è controllato attraverso autorizzazioni e le app si devono adeguare alle restrizioni che riguardano l'uso dei dati. Le app non sono ad esempio autorizzate ad utilizzare i dati sanitari a fini pubblicitari. Inoltre viene loro richiesto di fornire agli utenti le informazioni relative alla politica sulla privacy, in cui si espone come vengono usati i dati sanitari.

L'accesso ai dati sanitari da parte delle app è controllato dalle impostazioni sulla privacy dell'utente. Agli utenti viene chiesto di concedere l'accesso ai dati sanitari quando le app lo richiedono, così come accade anche per Contatti, Foto e altre sorgenti di dati in iOS. Tuttavia, nel caso dei dati sanitari, alle app viene concesso un accesso separato per la lettura e la scrittura dei dati, e un altro distinto per ogni tipo di informazione sanitaria. Gli utenti possono visualizzare e revocare, nel pannello Fonti dell'app Salute, i permessi precedentemente concessi per accedere ai dati sanitari.

Se alle app è stato consentito di scrivere i dati, significa anche che possono leggere quelli scritti da loro. Se è stato loro consentito di leggere i dati, possono leggere quelli scritti da tutte le fonti. Le app non possono tuttavia determinare l'accesso consentito ad altre app. Inoltre, non sono in grado di sapere in modo definitivo se è stato loro concesso l'accesso per la lettura dei dati sanitari. Quando un'app non dispone dell'accesso alla lettura, tutte le richieste non restituiranno alcun dato come risposta (la stessa risposta che darebbe un database vuoto). Questo fa sì che le app non possano dedurre lo stato di salute dell'utente leggendo i tipi di dati di cui sta tenendo traccia.

Cartella clinica

L'app Salute dà all'utente l'opzione di riempire una cartella clinica con le informazioni che potrebbero essere importanti nel caso di un'emergenza medica. Le informazioni sono inserite o aggiornate manualmente e non vengono sincronizzate con quelle disponibili nei database sanitari.

Le informazioni della cartella clinica possono essere visualizzate toccando il pulsante Emergenza in "Blocco schermo". Le informazioni sono archiviate sul dispositivo utilizzando la classe di protezione dati "Nessuna protezione" affinché possano essere accessibili senza dover inserire il codice del dispositivo. La cartella clinica è una funzionalità opzionale che permette agli utenti di trovare il giusto equilibrio tra sicurezza e privacy. Questi dati vengono inclusi nei backup di iCloud e non sono sincronizzati tra dispositivi che utilizzano CloudKit.

ReplayKit

ReplayKit è un framework che consente agli sviluppatori di aggiungere possibilità di registrazione e trasmissione live alle app. Inoltre, consente agli utenti di commentare le registrazioni e le trasmissioni utilizzando la videocamera anteriore e il microfono del dispositivo.

Registrazione di filmati

Nella registrazione di un filmato sono integrati vari livelli di sicurezza:

- **Finestra di dialogo con richiesta di permesso:** prima che la registrazione abbia inizio, ReplayKit visualizza un avviso in cui viene richiesto all'utente di dare il proprio consenso per la registrazione dello schermo e per l'uso del microfono e della fotocamera anteriore. Tale avviso viene presentato una sola volta per ogni processo dell'app; se l'app viene lasciata in background per più di 8 minuti, l'avviso viene visualizzato nuovamente.
- **Registrazione di schermo e audio:** la registrazione dello schermo e dell'audio avviene al di fuori del processo dell'app nel daemon *replayd* di ReplayKit. In questo modo viene garantito che il contenuto della registrazione non sia mai accessibile al processo dell'app.
- **Creazione e archiviazione di un filmato:** il file del filmato è scritto in una directory che è accessibile unicamente ai sottosistemi di ReplayKit e non è accessibile alle app. In questo modo viene impedito che le registrazioni possano essere utilizzate da terze parti senza il consenso dell'utente.
- **Anteprima e condivisione dell'utente finale:** l'utente dispone della possibilità di visualizzare in anteprima il filmato e di condividerlo con la UI di ReplayKit. La UI è presentata al di fuori del processo tramite l'infrastruttura delle estensioni di iOS e ha accesso al file del filmato generato.

Trasmissione

- **Registrazione di schermo e audio:** il meccanismo di registrazione dello schermo e dell'audio durante la trasmissione è identico a quello della registrazione dei filmati e avviene in *replayd*.
- **Estensioni di trasmissione:** perché i servizi di terze parti partecipino alla trasmissione di ReplayKit, devono creare due nuove estensioni configurate con l'endpoint com.apple.broadcast-services:
  - Un'estensione UI che consenta all'utente di configurare la trasmissione.
  - Un'estensione di upload che gestisca gli upload dei dati di video e audio sui server di back-end del servizio.

L'architettura garantisce che l'hosting delle app non offra privilegi riguardo ai contenuti audio e video trasmessi: vi avranno accesso solo ReplayKit e le estensioni di trasmissione di terze parti.

- **Selezione trasmissione:** per selezionare il servizio di trasmissione da utilizzare, ReplayKit fornisce un controller di visualizzazione (simile a UIActivityViewController) che lo sviluppatore può presentare nell'app. Il controller di visualizzazione è implementato tramite la SPI UIRemoteViewController ed è un'estensione che risiede all'interno del framework di ReplayKit. Si trova al di fuori del processo dell'app di hosting.
- **Selettore trasmissione di sistema:** consente agli utenti di avviare una trasmissione di sistema direttamente dall'app utilizzando la stessa interfaccia utente definita dal sistema che è accessibile tramite Centro di Controllo. L'interfaccia utente è implementata tramite la SPI UIRemoteViewController ed è un'estensione che risiede all'interno del framework di ReplayKit. Si trova al di fuori del processo dell'app di hosting.
- **Estensione di upload:** l'estensione di upload implementata dai servizi di trasmissione di terze parti per la gestione dei contenuti video e audio durante la trasmissione può scegliere di ricevere i contenuti in due modi:
  - Clip MP4 codificati di piccole dimensioni.
  - Buffer campione raw non codificati.
    - **Gestione dei clip MP4:** durante questa modalità di gestione, i clip codificati di piccole dimensioni vengono generati da *replayd* e archiviati in una posizione privata, accessibile unicamente ai sottosistemi di ReplayKit. Una volta generato il clip, *replayd* ne trasmetterà la posizione all'estensione di caricamento di terze parti tramite la SPI di richiesta NSExtension (basata su XPC). *replayd* genera anche un token sandbox di un solo uso che viene trasmesso all'estensione di upload per consentire a all'estensione di accedere a quel particolare clip filmato durante la richiesta dell'estensione.
    - **Gestione di buffer campione:** durante questa modalità di gestione, i dati video e audio vengono serializzati e passati all'estensione di upload di terze parti in tempo reale mediante una connessione diretta XPC. I dati video vengono codificati estraendo l'oggetto IOSurface dal buffer campione del video, codificandolo in modo sicuro come oggetto XPC, inviandolo quindi all'estensione di terze parti via XPC e decodificandolo infine nuovamente in modo sicuro nell'oggetto IOSurface.

Protezione note

L'app Note include una funzionalità di protezione delle note che consente agli utenti di proteggere il contenuto di determinate note. Le note protette vengono codificate tramite una frase chiave fornita dall'utente, che viene richiesta per visualizzare le note su iOS, macOS e sul sito web di iCloud.

Quando un utente protegge una nota a partire dalla frase chiave dell'utente viene generata una chiave a 16 byte tramite PBKDF2 e SHA256. Il contenuto della nota è codificato tramite AES-GCM. Nei dati core e in CloudKit vengono creati dei record per l'archiviazione della nota codificata, del tag, del vettore di inizializzazione, mentre i record della nota originale vengono eliminati; i dati codificati non vengono scritti in loro sostituzione. Anche gli allegati vengono codificati nello stesso modo. I tipi di allegato supportati includono immagini, disegni, tabelle, mappe e siti web. Le note con altri tipi di allegati non potranno essere codificate e gli allegati non supportati non potranno essere aggiunti alle note protette.

Quando un utente inserisce la frase chiave corretta per visualizzare o creare una nota protetta, Note si apre in una sessione protetta. Mentre l'app è aperta in questa modalità, all'utente non viene chiesto di inserire la frase chiave o di utilizzare Touch ID o Face ID per visualizzare o proteggere altre note. Tuttavia, se per alcune note è stata impostata una password diversa, nella sessione sicura saranno visualizzate unicamente le note protette tramite la password attuale. La sessione protetta viene chiusa quando:

- L'utente tocca il pulsante “Proteggi ora” in Note.
- Note viene messa in background per più di 3 minuti.
- Il dispositivo si blocca.

Gli utenti che dimenticano la password potranno comunque visualizzare le note protette o aggiungerne altre se hanno abilitato Touch ID o Face ID sui propri dispositivi. Inoltre, dopo tre tentativi non riusciti di inserimento della password, Note mostrerà un suggerimento fornito dall'utente. Per potere cambiare la password attuale, l'utente deve conoscerla.

Gli utenti possono reimpostare la password qualora abbiano dimenticato quella attuale. Questa funzionalità consente agli utenti di creare nuove note protette con una password nuova, ma non consente loro di visualizzare le note protette in precedenza. Tali note potranno essere visualizzate se verrà ricordata la password utilizzata per proteggerle. Per reimpostare la password è necessaria la password dell'account di iCloud dell'utente.

Note condivise

Le note possono essere condivise con altri. Le note condivise non usufruiscono della codifica end-to-end. Apple utilizza il tipo di dati codificati di CloudKit per qualsiasi testo o allegato inserito dall'utente in una nota. Le risorse sono sempre codificate con una chiave che è codificata in CKRecord. I metadati, come le date di creazione e modifica, non sono codificati. CloudKit gestisce il processo che consente agli utenti di codificare/decodificare i dati altrui.

Apple Watch

Apple Watch utilizza le funzionalità e le tecnologie di sicurezza sviluppate per iOS per proteggere non solo i dati sul dispositivo, ma anche le comunicazioni con il dispositivo iPhone abbinato e con Internet. Tali funzionalità e tecnologie includono la protezione dei dati e il controllo degli accessi al portachiavi. Inoltre, il codice dell'utente viene legato all'UID del dispositivo per creare chiavi di codifica.

L'abbinamento di Apple Watch e iPhone è protetto utilizzando un processo OOB (out-of-band) per scambiare le chiavi pubbliche, seguite dal segreto condiviso del collegamento Bluetooth Low Energy (BTLE). Apple Watch mostra un motivo animato, che viene acquisito dalla fotocamera di iPhone. Tale motivo contiene un segreto codificato che consente l'abbinamento OOB per BTLE 4.1. Se necessario, come metodo di abbinamento alternativo può essere usato un codice BTLE standard.

Una volta che la sessione Bluetooth Low Energy è stabilita e codificata tramite il protocollo di maggiore sicurezza disponibile nelle specifiche Bluetooth, Apple Watch e iPhone scambiano le chiavi utilizzando un processo adattato dal servizio di identificazione Apple, come descritto sotto “iMessage” nella sezione “Servizi Internet” di questo documento. Dopo lo scambio delle chiavi, la chiave di sessione Bluetooth viene eliminata e tutte le comunicazioni fra Apple Watch e iPhone vengono codificate via IDS; per fornire un secondo livello di protezione, i collegamenti Bluetooth, Wi-Fi e cellulare sono codificati. L'indirizzo di Bluetooth Low Energy viene modificato a rotazione a intervalli di 15 minuti per ridurre il rischio di compromissione del traffico.

Per supportare le app che devono trasmettere dati, la codifica viene fornita secondo i metodi descritti in “FaceTime”, nella sezione di questo documento dedicata ai servizi Internet, mediante il servizio IDS dell'iPhone abbinato o mediante una connessione a Internet diretta.

Apple Watch utilizza la codifica hardware dell'archiviazione e la protezione basata su classi per file ed elementi del portachiavi, come descritto nella sezione “Codifica e protezione dei dati” di questo documento, nonché keybag con controllo degli accessi per gli elementi del portachiavi. Anche le chiavi usate per le comunicazioni tra Apple Watch e iPhone sono tutelate dal sistema di protezione basato su classi.

Quando Apple Watch non si trova all'interno della copertura Bluetooth, può essere utilizzata la connessione Wi-Fi o cellulare. Apple Watch si collega automaticamente alle reti Wi-Fi alle quali l'iPhone abbinato si è già connesso e le cui credenziali sono state sincronizzate su Apple Watch mentre entrambi i dispositivi si trovavano a distanza di copertura. Questo comportamento di connessione automatica può essere configurato rete per rete nella sezione Wi-Fi dell'app Impostazioni di Apple Watch. È possibile accedere manualmente alle reti Wi-Fi a cui non è mai stata effettuata una connessione da nessuno dei due dispositivi tramite la sezione Wi-Fi dell'app Impostazioni di Apple Watch.

Quando Apple Watch e iPhone sono fuori distanza di copertura, Apple Watch si connette direttamente ai server di iCloud e di Gmail per scaricare la posta, piuttosto che sincronizzare i dati di Mail con l'iPhone abbinato tramite Internet. Per gli account Gmail, l'utente deve eseguire l'autenticazione a Google nella sezione Mail dell'app Watch su iPhone. Il token OAuth ricevuto da Google verrà inviato a Apple Watch in formato

codificato tramite il servizio di autenticazione Apple, in modo che possa essere utilizzato per scaricare la posta. Questo token OAuth non viene mai utilizzato per la connessione al server Gmail dall'iPhone abbinato.

È possibile bloccare manualmente Apple Watch tenendo premuto il tasto laterale. Inoltre, se il rilevamento del polso non è disattivato, il dispositivo si blocca automaticamente poco dopo essere stato rimosso dal polso dell'utente. Quando Apple Watch è bloccato, Apple Pay può essere utilizzato solo inserendo il codice dell'orologio. Il rilevamento del polso si disattiva dall'app Apple Watch su iPhone e può essere applicato tramite una soluzione MDM.

Anche il dispositivo iPhone abbinato può sbloccare Apple Watch, a patto che l'utente indossi l'orologio. In questo caso lo sblocco avviene instaurando una connessione autenticata dalle chiavi stabilite in fase di abbinamento: iPhone invia la chiave e l'orologio la utilizza per sbloccare le proprie chiavi di protezione dati. Il codice di Apple Watch non è noto a iPhone e non viene trasmesso. Questa funzionalità può essere disattivata dall'app Apple Watch su iPhone.

Apple Watch può essere abbinato con un solo iPhone alla volta. Quando viene annullato l'abbinamento, iPhone comunica l'istruzione di inizializzare tutti i contenuti e i dati da Apple Watch.

Apple Watch può essere configurato per effettuare un aggiornamento del software di sistema la notte stessa. Per ulteriori informazioni sul modo in cui il codice di Apple Watch viene archiviato per essere utilizzato durante l'aggiornamento, consulta la sezione dedicata alle keybag di questo documento.

Se sul dispositivo iPhone abbinato viene abilitato “Trova il mio iPhone”, viene abilitato anche l'uso del blocco attivazione su Apple Watch. “Blocco attivazione” rende più difficile l'utilizzo o la vendita di un orologio Apple Watch smarrito o rubato. “Blocco attivazione” richiede l'ID Apple e la password dell'utente per annullare l'abbinamento, inizializzare o riattivare Apple Watch.

Sicurezza della rete

Oltre alle misure di sicurezza integrate messe in pratica da Apple per proteggere i dati archiviati sui dispositivi iOS, le aziende possono implementarne molte altre per ottenere un grado maggiore di protezione delle informazioni che vengono trasmesse da e verso un dispositivo iOS.

Gli utenti di dispositivi mobili devono poter accedere a reti aziendali da qualsiasi parte del mondo, è quindi importante assicurarsi che siano autorizzati e che i loro dati siano protetti durante la trasmissione. iOS utilizza protocolli di rete standard, a cui gli sviluppatori hanno accesso, per le comunicazioni autenticate, autorizzate e codificate. iOS integra tecnologie collaudate e gli ultimi standard per raggiungere questi obiettivi di sicurezza, sia per le connessioni a reti Wi-Fi che per quelle a reti dati cellulari.

Su altre piattaforme è necessario un software firewall per proteggere da eventuali intrusioni le porte di comunicazione aperte. Sui dispositivi iOS non è invece necessario alcun software firewall aggiuntivo, in quanto iOS riesce a ridurre la possibilità di attacchi limitando le porte di ascolto e rimuovendo utility di rete non necessarie, quali ad esempio telnet, shell o web server.

TLS

iOS supporta Transport Layer Security (TLS 1.0, TLS 1.1, TLS 1.2) e DTLS. Supporta sia AES-128 e AES-256 e predilige suite di cifratura con proprietà di perfect forward secrecy. Safari, Calendario, Mail e altre app Internet avviano automaticamente questo protocollo per instaurare un canale di comunicazione codificato tra il dispositivo e i servizi di rete. Le API di alto livello (come CFNetwork) rendono facile l'adozione di TLS nelle app da parte degli sviluppatori, mentre quelle di basso livello (Network. framework) forniscono un controllo dettagliato. CFNetwork disattiva SSLv3 e alle app che utilizzano WebKit (come Safari) non è consentito stabilire connessioni SSLv3.

In iOS 11 o versioni successive e macOS High Sierra o versioni successive, i certificati SHA-1 non sono più consentiti per le connessioni TLS, a meno che non siano segnalati come attendibili dall'utente. Inoltre, non sono consentiti neanche i certificati con chiavi RSA inferiori ai 2048 bit. La suite di cifratura simmetrica RC4 è sconsigliata in iOS 10 e macOS Sierra. Di default, i client o server TLS sui cui sono implementati le API SecureTransport non hanno le suite di cifratura RC4 abilitate e non possono connettersi quando RC4 è l'unica suite di cifratura disponibile. Per sicurezza, i servizi e le app che richiedono RC4 devono essere aggiornati per potere utilizzare le suite di cifratura più recenti e sicure. In iOS 12.1, i certificati emessi dopo il 15 ottobre 2018 da un certificato root considerato attendibile dal sistema devono essere inseriti in un log attendibile per la trasparenza dei certificati affinché possano effettuare connessioni TLS.

Sicurezza dei trasferimenti delle app

App Transport Security garantisce requisiti di connessione di default che assicurano il rispetto da parte delle app delle linee guida per le connessioni sicure durante l'utilizzo delle API NSURLConnection, CFURL o NSURLSession. In maniera predefinita, App Transport Security limita la selezione di cifratura perché includa solo suite che forniscono forward secrecy, in particolare ECDHE_ECDSA_AES e ECDHE_RSA_AES in modalità GCM o CBC. Le app sono in grado di disabilitare il requisito di forward secrecy per dominio; in quel caso, RSA_AES viene aggiunto all'insieme delle cifrature disponibili.

I server devono supportare TLS 1.2 e il forward secrecy; i certificati devono essere validi e firmati tramite funzioni uguali o superiori a SHA-256 con chiavi uguali o superiori a RSA a 2048 bit o a curva ellittica a 256 bit.

Le connessioni di rete che non soddisfano tali requisiti non verranno stabilite, a meno che l'app non ignori App Transport Security. La presenza di certificati non validi comporta sempre un'interruzione forzata e un blocco della connessione. App Transport Security viene applicato automaticamente alle app realizzate per iOS 9 o successivo.

VPN

I servizi di rete sicura come VPN (Virtual Private Networking) richiedono delle impostazioni e una configurazione minima per poter funzionare con i dispositivi iOS. I dispositivi iOS funzionano con i server VPN che supportano i seguenti protocolli e metodi di autenticazione:

- IKEv2/IPSec con autenticazione tramite segreto condiviso, certificati RSA, certificati **ECDSA**, EAP-MSCHAPv2 o EAP-TLS.
- SSL-VPN con l'app client adeguata scaricata da App Store.
- Cisco IPSec con autenticazione utente tramite password e autenticazione automatica mediante segreto condiviso e certificati.
- L2TP/IPSec con autenticazione utente tramite password MS-CHAPV2 e autenticazione automatica mediante segreto condiviso.

iOS supporta:

- **La connessione VPN su richiesta** per le reti che utilizzano l'autenticazione basata sui certificati. Le politiche IT specificano quali sono i domini che richiedono una connessione VPN utilizzando un apposito profilo di configurazione.
- **La connessione VPN per app**, che facilita le connessioni VPN su base molto più dettagliata. Una soluzione MDM può specificare una connessione per ogni app gestita e/o domini specifici di Safari. Questa funzione garantisce che i dati protetti passino sempre attraverso le reti aziendali, a differenza dei dati personali dell'utente.
- **La connessione VPN sempre attiva**, che può essere configurata per i dispositivi gestiti tramite soluzione MDM e supervisionati utilizzando Apple Configurator 2, Apple School Manager o Apple Business Manager. In questo modo l'utente non dovrà più attivare la VPN per abilitare la protezione quando si connette a reti cellulari o Wi-Fi. La VPN sempre attiva fa in modo che l'azienda abbia il pieno controllo sul traffico dei dispositivi, attraverso il tunneling di tutto il traffico IP verso l'azienda. Il protocollo di tunneling di default, IKEv2, protegge la trasmissione del traffico attraverso la codifica dei dati. L'azienda può dunque monitorare e filtrare il traffico tra i dispositivi, proteggere i dati all'interno della propria rete e limitare l'accesso a Internet dei dispositivi.

Wi-Fi

iOS supporta i protocolli Wi-Fi che costituiscono lo standard di settore, incluso WPA2 Enterprise, per fornire accesso autenticato alle reti wireless aziendali. WPA2 Enterprise utilizza la codifica AES a 128 bit, un metodo di codifica che fornisce il massimo livello di protezione dei dati durante l'invio e la ricezione di comunicazioni attraverso una connessione di rete Wi-Fi. Grazie al supporto di 802.1X, i dispositivi iOS possono essere integrati in un'ampia gamma di ambienti di autenticazione RADIUS. I metodi di autenticazione wireless 802.1X supportati da iPhone e iPad comprendono: EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, PEAPv1 e LEAP.

Oltre alla protezione dei dati, iOS amplia la protezione di livello WPA2 alla gestione dei pacchetti unicast e multicast mediante il servizio Protected Management Frame a cui si fa riferimento in 802.11w. Il supporto PMF è disponibile su iPhone 6 e iPad Air 2 o modelli successivi.

Quando analizza la connessione Wi-Fi senza essere associato a una rete Wi-Fi, iOS utilizza un indirizzo MAC (Media Access Control) casuale. Tale analisi può essere effettuata per trovare la rete Wi-Fi preferita e connettersi ad essa oppure per aiutare i servizi di localizzazione per le app che utilizzano i recinti geografici, come i promemoria basati sulla posizione, o per correggere una posizione in Mappe di Apple. Le analisi Wi-Fi che si verificano durante il tentativo di connessione alla rete Wi-Fi preferita non avvengono tramite indirizzi casuali.

iOS utilizza un indirizzo MAC casuale anche durante le scansioni ePNO (enhanced Preferred Network Offload) quando un dispositivo non è associato a una rete Wi-Fi e il suo processore è in stop. Le scansioni ePNO sono eseguite quando il dispositivo utilizza i servizi di localizzazione per le app che usano recinti geografici, come ad esempio i promemoria basati sulla posizione che determinano se il dispositivo si trova nei pressi di un luogo specifico.

Considerando che adesso l'indirizzo MAC di un dispositivo cambia se il dispositivo viene disconnesso da una rete Wi-Fi, non potrà essere utilizzato per seguire continuamente la posizione di un dispositivo da parte di osservatori passivi del traffico Wi-Fi, nemmeno quando il dispositivo è connesso a una rete cellulare. Apple ha informato i produttori di Wi-Fi del fatto che le scansioni di iOS utilizzano indirizzi MAC casuali e che né Apple né i produttori possono predire tali indirizzi. Gli indirizzi MAC Wi-Fi casuali non sono supportati su iPhone 4s o precedenti.

Su iPhone 6s o modelli successivi, la proprietà nascosta di una rete Wi-Fi conosciuta è nota e viene aggiornata automaticamente. Se il SSID (Service Set Identifier) di una rete Wi-Fi viene trasmesso, il dispositivo iOS non lo includerà nella richiesta, in modo da impedire la trasmissione del nome di reti non nascoste.

Per proteggere il dispositivo da vulnerabilità nel firmware del processore di rete, le interfacce come Wi-Fi e baseband hanno accesso limitato alla memoria del processore per le applicazioni. Quando la comunicazione con il processore di rete avviene tramite le interfacce USB o SDIO, il processore di rete non può instaurare transazioni DMA (Direct Memory Access) con il processore per le applicazioni. Quando viene utilizzata l'interfaccia PCIe, ciascun processore di rete si trova sul proprio bus PCIe isolato. Un IOMMU su ciascun bus PCIe limita l'accesso DMA del processore alle pagine della memoria contenenti i pacchetti della rete o le strutture di controllo.

Bluetooth

Il supporto Bluetooth su iOS è stato progettato per fornire una funzionalità utile senza richiedere un accesso maggiore e non necessario ai dati privati. I dispositivi iOS supportano le connessioni Encryption Mode 3, Security Mode 4 e Service Level 1. iOS supporta i seguenti profili Bluetooth:

- HFP (Hands-Free Profile)
- PBAP (Phone Book Access Profile)
- MAP (Message Access Profile)
- A2DP (Advanced Audio Distribution Profile)
- AVRCP (Audio/Video Remote Control Profile)
- PAN (Personal Area Network Profile)
- HID (Human Interface Device Profile)

Il supporto per ognuno di questi profili varia a seconda del dispositivo.

Per ulteriori informazioni, consulta: https://support.apple.com/HT3647

Single Sign-on

iOS supporta l'autenticazione alle reti aziendali attraverso SSO (Single Sign-on). SSO funziona con le reti basate su Kerberos per autenticare gli utenti ai servizi a cui sono stati autorizzati ad accedere. La tecnologia SSO può essere utilizzata per una serie di attività di rete, che spazia dalle sessioni sicure di Safari ad app di terze parti. È inoltre supportata l'autenticazione basata su certificati (PKINIT).

SSO di iOS utilizza i token SPNEGO e il protocollo HTTP Negotiate, grazie ai quali può lavorare con gateway di autenticazione basati su Kerberos e con sistemi di autenticazione integrata Windows (Windows Integrated Authentication) che supportano i ticket Kerberos. Il supporto SSO si basa sul progetto open source Heimdal.

Sono supportati i seguenti tipi di codifica:

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

Safari supporta SSO e anche le app di terze parti che usano API di networking iOS standard possono essere configurate per poter utilizzare questa tecnologia. Per la configurazione SSO, iOS supporta un payload di un profilo di configurazione che consente alle soluzioni MDM di scaricare le impostazioni necessarie. Si tratta dunque di impostare il nome principale dell'utente (cioè, l'account utente Active Directory), le impostazioni realm di Kerberos e di indicare le app e URL di Safari a cui è consentito l'uso del SSO.

Continuity

Continuity sfrutta tecnologie come iCloud, Bluetooth e Wi-Fi per consentire agli utenti di riprendere su un dispositivo l'attività cominciata su un altro, di fare e ricevere telefonate, di inviare e ricevere messaggi di testo e di condividere una connessione cellulare a Internet.

Handoff

Con Handoff, quando il Mac e i dispositivi iOS dell'utente sono vicini, l'utente può trasferire automaticamente ciò a cui sta lavorando da un dispositivo all'altro. Handoff permette all'utente di cambiare dispositivo continuando immediatamente a lavorare.

Quando l'utente accede a iCloud su un secondo dispositivo con funzionalità Handoff, i due dispositivi stabiliscono un abbinamento fuori banda con Bluetooth Low Energy 4.2 utilizzando il servizio Apple Push Notification (APN). I singoli messaggi sono codificati in modo simile a quanto avviene per iMessage. Una volta completato l'abbinamento, i due dispositivi generano una chiave simmetrica AES a 256 bit che viene archiviata nel portachiavi del dispositivo. Questa chiave può codificare e autenticare le trasmissioni Bluetooth Low Energy, che comunicano l'attività corrente del dispositivo ad altri dispositivi abbinati via iCloud utilizzando AES-256 in modalità GCM, con misure di sicurezza contro i replay attack.

La prima volta che riceve una trasmissione da una nuova chiave, il dispositivo instaura una connessione Bluetooth Low Energy con il dispositivo di origine ed effettua uno scambio della chiave di codifica della trasmissione. Questa connessione è protetta grazie alla codifica standard Bluetooth Low Energy 4.2 e alla codifica dei singoli messaggi, in maniera simile a quanto avviene per i messaggi iMessage. In alcune situazioni, i messaggi viaggiano attraverso il servizio APN anziché via Bluetooth Low Energy. Il payload dell'attività è protetto e trasferito come avviene per iMessage.

Handoff fra app native e siti web

Handoff consente alle app native per iOS di riprendere le pagine web in domini legittimamente controllati dallo sviluppatore dell'app. Permette inoltre di riprendere in un browser l'attività svolta dall'utente nell'app nativa.

Per impedire alle app native di riprendere i siti web non controllati dallo sviluppatore, l'app deve dimostrare di avere un legittimo controllo sui domini web in questione. Il controllo su un sito web si stabilisce attraverso il meccanismo utilizzato per le credenziali web condivise. Per i dettagli, consulta “Accesso delle app alle password salvate” nella sezione “Codifica e protezione dati” di questo documento. Il sistema deve convalidare il controllo dell'app sul nome di dominio prima che sia consentito all'app di accettare l'attività dell'utente via Handoff.

La sorgente di una pagina web trasferita tramite Handoff può essere qualsiasi browser che abbia adottato le API di Handoff. Quando l'utente visualizza una pagina web, il sistema annuncia il nome di dominio della pagina nei byte di trasmissione codificati di Handoff. Solo gli altri dispositivi dell'utente possono decodificare i byte di trasmissione (come descritto in precedenza in questa sezione).

Sul dispositivo ricevente, il sistema rileva che un'app nativa installata accetta il trasferimento Handoff dal nome di dominio annunciato e visualizza l'icona di quell'app nativa come opzione Handoff. Quando viene avviata, l'app nativa riceve l'URL completo e il titolo della pagina web. Fra il browser e l'app nativa non vengono trasferite altre informazioni.

Nella direzione opposta, un'app nativa può specificare un URL alternativo quando un dispositivo che riceve il trasferimento Handoff non dispone della stessa app. In questo caso il sistema visualizza il browser di default dell'utente come opzione Handoff (se tale browser ha adottato le API di Handoff). Quando si richiede il trasferimento Handoff, il browser viene avviato e riceve l'URL alternativo fornito dall'app sorgente. Non è necessario che l'URL alternativo rientri nei nomi di dominio controllati dallo sviluppatore dell'app nativa.

Handoff con volumi elevati di dati

Oltre alle funzionalità di base di Handoff, alcune app possono utilizzare API che supportano l'invio di un volume maggiore di dati attraverso una tecnologia Wi-Fi peer-to-peer creata da Apple (simile a AirDrop). Ad esempio, l'app Mail utilizza queste API per consentire il trasferimento via Handoff di una bozza, che può contenere allegati di grandi dimensioni.

Quando un'app utilizza questa capacità, lo scambio fra i due dispositivi ha inizio proprio come in Handoff (vedi le sezioni precedenti). Tuttavia, dopo aver ricevuto il payload iniziale via Bluetooth Low Energy, il dispositivo ricevente avvia una nuova connessione Wi-Fi. La connessione è codificata (TLS) e prevede lo scambio dei certificati di identità iCloud, che saranno verificati confrontandoli con l'identità dell'utente. Su questa connessione codificata vengono quindi trasferiti ulteriori dati di payload fino a completare il trasferimento.

Appunti universali

Gli appunti universali si servono di Handoff per trasferire in modo sicuro il contenuto degli appunti tra i dispositivi, perché sia possibile copiare da un dispositivo e incollare su un altro. I contenuti sono protetti nello stesso modo degli altri dati di Handoff e vengono condivisi di default con gli appunti universali, salvo nel caso in cui lo sviluppatore decida di non consentire la condivisione.

Le app hanno accesso ai dati degli appunti a prescindere dal fatto che l'utente abbia incollato o meno gli appunti nell'app. Con gli appunti universali, l'accesso a tali dati viene esteso alle app presenti sugli altri dispositivi (associati allo stesso account di iCloud).

Sblocco automatico

I computer Mac che supportano lo sblocco automatico utilizzano Bluetooth Low Energy e la rete Wi-Fi peer-to-peer per consentire all'utente lo sblocco del Mac in modo sicuro tramite Apple Watch. Ogni Mac e Apple Watch associato a un account iCloud deve utilizzare l'autenticazione a due fattori.

Quando abiliti un Apple Watch per sbloccare un Mac, viene stabilita una connessione sicura utilizzando le identità per lo sblocco automatico. Il Mac crea un segreto di sblocco casuale valido per un solo uso e lo trasmette ad Apple Watch tramite questa connessione. Il segreto viene conservato in Apple Watch e sarà accessibile solo quando Apple Watch è sbloccato (consulta “Classi di protezione dei dati” nella sezione “Codifica e protezione dati”). Il nuovo segreto non può essere la password dell'utente.

Durante un'operazione di sblocco, il Mac utilizza Bluetooth Low Energy per creare una connessione con Apple Watch. A questo punto viene stabilita una connessione protetta tra i due dispositivi tramite le chiavi condivise utilizzate quando è stato abilitato lo sblocco automatico. Il Mac e Apple Watch utilizzano quindi la connessione Wi-Fi peer-to-peer e una chiave sicura derivata dalla connessione protetta per determinare la distanza tra i due dispositivi. Se i dispositivi si trovano l'uno nel raggio di portata dell'altro, la connessione protetta è usata per trasferire il segreto pre-condiviso per sbloccare il Mac. Una volta che lo sblocco è avvenuto correttamente, il Mac sostituisce il segreto di sblocco attuale con un nuovo segreto di sblocco valido per un solo uso e lo trasmette a Apple Watch utilizzando la connessione.

Inoltro delle chiamate cellulari tramite iPhone

Quando il Mac, iPad o iPod touch si trovano sulla stessa rete Wi-Fi di iPhone, possono essere utilizzati per effettuare e ricevere chiamate telefoniche tramite la connessione cellulare di iPhone. Per la configurazione è necessario che sui dispositivi sia stato effettuato l'accesso sia a iCloud che a FaceTime utilizzando lo stesso ID Apple.

Quando arriva una chiamata in entrata, tutti i dispositivi configurati riceveranno una notifica tramite il **servizio Apple Push Notification (APN)**. Ogni notifica utilizzerà la stessa codifica end-to-end di iMessage. I dispositivi che sono sulla stessa rete mostreranno una notifica di chiamata in entrata. Quando l'utente risponde, l'audio verrà trasmesso direttamente da iPhone utilizzando una connessione peer-to-peer sicura fra i due dispositivi.

Quando l'utente risponde a una chiamata su uno dei dispositivi, i dispositivi nelle vicinanze abbinati tramite iCloud smetteranno di suonare dopo una breve trasmissione via Bluetooth Low Energy. I byte di tale notifica sono codificati con lo stesso metodo con cui vengono annunciati i trasferimenti di Handoff.

Anche le chiamate in uscita vengono inoltrate a iPhone tramite il servizio di notifiche push di Apple e l'audio verrà trasmesso nella stessa maniera sul collegamento peer-to-peer sicuro fra i dispositivi.

Gli utenti possono disabilitare l'inoltro delle chiamate disattivando l'opzione “Chiamate cellulare iPhone” nelle impostazioni di FaceTime.

Inoltro messaggi di testo tramite iPhone

L'inoltro dei messaggi di testo invia automaticamente i messaggi di testo ricevuti su iPhone al Mac, iPad o iPod touch registrati dell'utente. Su ogni dispositivo deve essere stato effettuato l'accesso al servizio iMessage utilizzando lo stesso ID Apple. Quando l'inoltro dei messaggi di testo è attivato e l'autenticazione a due fattori è abilitata, la registrazione dei dispositivi che fanno parte di una cerchia di attendibilità dell'utente è automatica. Altrimenti, la registrazione viene verificata su ogni dispositivo inserendo un codice numerico causale a sei cifre generato da iPhone.

Una volta collegati i dispositivi, iPhone provvede a codificare gli SMS in entrata e li inoltra a ciascun dispositivo, utilizzando i metodi descritti nella sezione iMessage di questo documento. Le risposte sono inviate nuovamente a iPhone utilizzando lo stesso metodo, quindi iPhone le invia come messaggi di testo attraverso il meccanismo di trasmissione SMS del gestore. La funzionalità “Inoltro SMS” può essere disattivata nelle impostazioni di Messaggi.

Instant Hotspot

I dispositivi iOS che supportano Instant Hotspot utilizzano la tecnologia Bluetooth Low Energy per rilevare i dispositivi su cui è stato effettuato l'accesso allo stesso account iCloud e comunicare con loro. I computer Mac compatibili dotati di OS X Yosemite e versioni successive utilizzano la stessa tecnologia per rilevare e comunicare con i dispositivi iOS con Instant Hotspot.

Quando l'utente inserisce le impostazioni Wi-Fi sul dispositivo iOS, quest'ultimo emette una trasmissione Bluetooth Low Energy che contiene un identificatore concordato tra tutti i dispositivi su cui è stato effettuato l'accesso allo stesso account iCloud. L'identificatore è generato da un DSID (Destination Signaling Identifier) legato all'account iCloud e prevede una rotazione periodica. Se nelle vicinanze ci sono altri dispositivi su cui è stato effettuato l'accesso allo stesso account iCloud e che supportano l'hotspot personale, questi rilevano il segnale e rispondono indicando la loro disponibilità.

Quando l'utente sceglie un dispositivo, viene inviata una richiesta di attivare l'hotspot personale a quel dispositivo. La richiesta viaggia su un collegamento protetto dalla codifica standard di Bluetooth Low Energy ed è codificata in modo simile a quanto avviene per iMessage. Il dispositivo risponde quindi sullo stesso collegamento Bluetooth Low Energy utilizzando lo stesso tipo di codifica per messaggio e fornendo le informazioni sulla connessione con l'hotspot personale.

Sicurezza AirDrop

I dispositivi iOS che supportano AirDrop usano BLE (Bluetooth Low Energy) e la tecnologia Wi-Fi peer-to-peer creata da Apple per inviare file e informazioni ai dispositivi nelle vicinanze, compresi i computer Mac con OS X 10.11 o versione successiva che usano AirDrop. Il segnale Wi-Fi è usato per comunicare direttamente tra i dispositivi senza necessità di una connessione Internet o di un punto di accesso Wi-Fi.

Quando un utente abilita AirDrop, sul dispositivo viene archiviata un'identità RSA a 2048 bit. Inoltre, viene creato un hash di identità AirDrop in base agli indirizzi e-mail e ai numeri telefonici associati all'ID Apple dell'utente.

Quando un utente sceglie AirDrop come metodo di condivisione di un elemento, il dispositivo emette un segnale AirDrop attraverso Bluetooth Low Energy. Gli altri dispositivi nelle vicinanze che sono attivi e hanno AirDrop attivato rilevano il segnale e rispondono con una versione abbreviata dell'hash di identità dei rispettivi proprietari.

AirDrop è impostato di default per la condivisione con “Solo contatti”. Gli utenti possono inoltre decidere utilizzare AirDrop per la condivisione con tutti oppure se disattivare completamente tale funzione. Nella modalità “Solo contatti”, gli hash di identità ricevuti sono confrontati con quelli delle persone presenti nell'app Contatti dell'iniziatore. Se viene trovata una corrispondenza, il dispositivo di invio crea una rete Wi-Fi peer-to-peer e rende visibile la connessione AirDrop utilizzando Bonjour. I dispositivi di ricezione inviano i loro hash di identità completi all'iniziatore tramite questa connessione. Se l'hash completo corrisponde ancora alle informazioni in Contatti, il nome e la foto del destinatario (se presenti in Contatti) vengono visualizzati nella finestra di condivisione di AirDrop.

Utilizzando AirDrop, l'utente che esegue l'invio seleziona con chi desidera condividere le informazioni. Il dispositivo di invio avvia una connessione codificata (TLS) con il dispositivo di ricezione e avviene lo scambio i rispettivi certificati di identità iCloud. L'identità nei certificati è verificata confrontando le informazioni con i dati presenti nell'app Contatti di ogni utente. Successivamente, all'utente che riceve viene chiesto di accettare il trasferimento in entrata dalla persona o dispositivo identificati. Se sono stati selezionati più destinatari, questo processo viene ripetuto per ogni destinazione.

Il processo seguito nella modalità Tutti è lo stesso, ma se non viene trovata una corrispondenza in Contatti, i dispositivi di ricezione sono mostrati nella finestra di invio di AirDrop con una sagoma e con il nome del dispositivo, così come specificato in Impostazioni > Generali > Info > Nome.

Le organizzazioni possono limitare l'utilizzo di AirDrop per i dispositivi o le app gestite tramite una soluzione MDM.

Condivisione della password Wi-Fi

I dispositivi iOS che supportano la condivisione della password Wi-Fi utilizzano un meccanismo simile a AirDrop per inviare una password Wi-Fi da un dispositivo a un altro.

Quando un utente seleziona una rete Wi-Fi (richiedente) e viene richiesta la password Wi-Fi, il dispositivo Apple avvia una ricerca tramite Bluetooth Low Energy indicando che necessita della password Wi-Fi. Gli altri dispositivi Apple che sono attivi, nelle immediate vicinanze e che dispongono della password per la rete Wi-Fi selezionata si connettono tramite Bluetooth Low Energy al dispositivo richiedente.

Il dispositivo con la password Wi-Fi (concedente) chiede le informazioni di contatto del richiedente, che deve dimostrare la propria identità tramite un meccanismo simile a AirDrop. Una volta provata l'identità, il concedente invia al richiedente la PSK di 64 caratteri, che può essere utilizzata per accedere alla rete.

Le organizzazioni possono limitare l'utilizzo della condivisione della password Wi-Fi per i dispositivi o le app gestite tramite una soluzione MDM.

Apple Pay

Grazie a Apple Pay, gli utenti possono utilizzare i dispositivi iOS supportati, Apple Watch e il Mac per effettuare i pagamenti in modo facile, sicuro e privato sugli Store, nelle app e sul web in Safari. Gli utenti possono anche aggiungere le carte dei mezzi pubblici compatibili con Apple Pay a Wallet. È un metodo intuitivo e facile da usare ed è sviluppato con un sistema di sicurezza integrato a livello di hardware e di software.

Apple Pay è inoltre progettato per proteggere le informazioni personali dell'utente. Apple Pay non raccoglie alcuna informazione sulle transazioni che possa essere ricollegata all'utente. Le transazioni di pagamento vengono effettuate tra l'utente, il venditore e l'emittente della carta.

Componenti di Apple Pay

Secure Element: Secure Element è un processore certificato e realizzato secondo i massimi standard del settore. Su di esso è in esecuzione Java Card, una piattaforma che soddisfa i requisiti dell'industria finanziaria per i pagamenti elettronici.

Controller NFC: il controller NFC gestisce i protocolli Near Field Communication e instrada la comunicazione tra il processore per le applicazioni e Secure Element e tra Secure Element e il terminale POS.

Wallet: Wallet è utilizzato per aggiungere e gestire le carte di credito, di debito e le carte dei negozi e per eseguire pagamenti con Apple Pay. In Wallet gli utenti possono visualizzare le carte e informazioni aggiuntive fornite dall'emittente, come la politica sulla privacy dell'emittente, le transazioni recenti e molto altro ancora. Gli utenti possono anche aggiungere le carte a Apple Pay in:

- Impostazione Assistita e Impostazioni per iOS.
- L'app Watch per Apple Watch.
- Il pannello Wallet e Apple Pay di Preferenze di Sistema per il Mac.

Inoltre Wallet consente agli utenti di aggiungere e gestire carte dei mezzi pubblici, carte fedeltà, carte d'imbarco, biglietti, carte regalo, tessere identificative studente e altro ancora.

Secure Enclave: su iPhone, iPad e Apple Watch, Secure Enclave gestisce il processo di autenticazione e autorizza le transazioni.

Su Apple Watch, il dispositivo deve essere sbloccato e l'utente deve premere due volte il tasto laterale. Il doppio clic viene rilevato e inoltrato direttamente a Secure Element o Secure Enclave, dove disponibile, senza passare dal processore delle applicazioni.

Server Apple Pay: i server Apple Pay gestiscono la configurazione e l'inserimento delle carte di credito, carte di debito, carte dei mezzi pubblici e tessere identificative studente in Wallet e i numeri di account del dispositivo archiviati in Secure Element. Comunicano sia con il dispositivo sia con i server delle rete di pagamento o con i server degli emittenti delle carte. Sono inoltre responsabili di codificare nuovamente le credenziali di pagamento per le transazioni all'interno delle app.

Come viene utilizzato Secure Element da Apple Pay

All'interno di Secure Element è presente un apposito applet per la gestione di Apple Pay. Include anche degli applet certificati dalle reti di pagamento o dagli emittenti delle carte. I dati relativi alla carta di debito, di credito o prepagata vengono inviati codificati dalla rete di pagamento o dall'emittente della carta a questi applet utilizzando chiavi conosciute solo dalla rete di pagamento o degli emittenti delle carte e dal dominio di sicurezza degli applet. Questi dati sono archiviati all'interno degli applet e protetti utilizzando le funzionalità di sicurezza di Secure Element. Durante una transazione, il terminale comunica direttamente con Secure Element attraverso il controller NFC (Near Field Communication) mediante un bus hardware dedicato.

Come viene utilizzato il controller NFC da Apple Pay

Come gateway di Secure Element, il controller NFC garantisce che tutti i pagamenti contactless siano eseguiti utilizzando un terminale POS che si trovi in prossimità del dispositivo. Solo le richieste di pagamento provenienti da un terminale entro il raggio di azione sono contrassegnate dal controller NFC come transazioni contactless.

Una volta che il proprietario della carta ha autorizzato il pagamento della carta di credito, di debito o prepagata (comprese le carte dei negozi) usando Touch ID, Face ID o il codice, o premendo due volte il tasto laterale su Apple Watch dopo averlo sbloccato, le risposte contactless preparate dagli applet di pagamento all'interno di Secure Element sono dirette dal controller al campo NFC. Di conseguenza i dettagli di autorizzazione per il pagamento per le transazioni contactless sono contenuti nel campo NFC locale e non sono mai esposti al processore per le applicazioni. I dettagli di autorizzazione per il pagamento all'interno delle app e sul web vengono invece diretti al processore per le applicazioni, ma solo dopo la codifica eseguita da Secure Element sul server Apple Pay.

Aggiunta di carte di credito, di debito e prepagate

Quando un utente aggiunge a Wallet una carta di credito, di debito o prepagata (comprese le carte dei negozi), Apple invia i dati della carta, insieme a quelli relativi al dispositivo e al conto dell'utente, all'ente di emissione della carta o al fornitore di servizi autorizzato dall'ente di emissione della carta, il tutto in modalità sicura. Attraverso queste informazioni, l'emittente deciderà se approvare o meno l'aggiunta della carta a Wallet.

Apple Pay utilizza tre chiamate lato server per inviare e ricevere comunicazioni con l'emittente o la rete come parte del processo di inserimento delle carte: *Campi richiesti, Verifica carta* e *Collega e inserisci*. L'emittente o la rete utilizzano queste chiamate per verificare, approvare e aggiungere carte a Wallet. Queste sessioni client-server sono codificate tramite TLS 1.2.

I numeri completi delle carte non sono archiviati sul dispositivo o sui server Apple. In Secure Element, viene invece creato, codificato e poi archiviato un numero di account del dispositivo unico. Questo numero unico è codificato in modo che neanche Apple possa accedervi. Il numero di account del dispositivo è unico e diverso dai tipici numeri delle carte di credito o di debito; l'emittente o la rete di pagamento possono impedirne

l'utilizzo su una carta a banda magnetica, per telefono o sui siti web. Il numero di account del dispositivo in Secure Element è isolato da iOS e watchOS, non viene mai archiviato sui server di Apple Pay e non è mai sottoposto a backup su iCloud.

Le carte da utilizzare con Apple Watch si inseriscono in Apple Pay con l'app Watch su iPhone o tramite l'app per iPhone dell'emittente. Per poter inserire una carta per Apple Watch è necessario che l'orologio si trovi entro il raggio d'azione del Bluetooth. Le carte sono registrate specificamente per l'uso con Apple Watch e ciascuna ha un proprio numero di account del dispositivo, memorizzato in Secure Element su Apple Watch.

Quando le carte di credito, di debito o prepagate (comprese le carte dei negozi) vengono aggiunte, verranno visualizzate in un elenco durante Impostazione Assistita sui dispositivi in cui è stato effettuato l'accesso allo stesso account di iCloud. Tali carte restano nell'elenco finché risulteranno attive su almeno un dispositivo. Le carte vengono rimosse dall'elenco dopo essere state rimosse da tutti i dispositivi per sette giorni. Per questa funzionalità è necessario che sia abilitata l'autenticazione a due fattori sull'account di iCloud in questione.

Aggiunta manuale di una carta ad Apple Pay

Per facilitare l'inserimento manuale delle carte, vengono utilizzati il nome, il numero della carta, la data di scadenza e il CVV. Da Impostazioni, Wallet o l'app Apple Watch, gli utenti possono inserire manualmente le informazioni digitandole o utilizzando la fotocamera sul dispositivo. Quando la fotocamera acquisisce le informazioni della carta, Apple prova a inserire i dati nei campi del nome, numero della carta e data di scadenza. La foto non è mai salvata sul dispositivo né archiviata nella libreria fotografica. Una volta compilati tutti i campi, il processo di verifica della carta controlla tutti i campi tranne quello relativo al CVV. Questi dati vengono codificati e inviati al server Apple Pay.

Se il processo "Verifica carta" dà come risultato un ID di termini e condizioni, Apple scarica e mostra all'utente i termini e le condizioni dell'emittente della carta. Se l'utente accetta i termini e le condizioni, Apple invia al processo "Collega e inserisci" l'ID dei termini che sono stati accettati, insieme al CVV. Inoltre, nell'ambito del processo "Collega e inserisci", Apple condivide informazioni dal dispositivo con l'istituto o il circuito emittente, quali: informazioni sull'attività dell'account iTunes e App Store (ad esempio, se l'utente ha una lunga cronologia di transazioni su iTunes), informazioni sul dispositivo (ad esempio numero di telefono, nome e modello, nonché ogni eventuale dispositivo iOS abbinato necessario per configurare Apple Pay) e la posizione approssimativa nel momento in cui è stata aggiunta la carta (se i servizi di localizzazione sono attivi). Attraverso queste informazioni, l'emittente deciderà se approvare o meno l'aggiunta della carta ad Apple Pay.

Come risultato del processo "Collega e inserisci" si verificano due condizioni:

- Il dispositivo inizia a scaricare il biglietto di Wallet che rappresenta la carta di debito o di credito.
- Il dispositivo inizia a vincolare la carta a Secure Element.

Il file del biglietto contiene gli URL per scaricare l'immagine della carta, i metadati della carta come ad esempio le informazioni di contatto, la relativa app dell'emittente e le funzionalità supportate. Contiene anche lo stato del biglietto, che indica ad esempio se la personalizzazione di Secure Element è stata completata, se la carta è attualmente sospesa dall'istituto emittente o se sono necessarie ulteriori informazioni prima che la carta possa essere utilizzata per effettuare pagamenti con Apple Pay.

Aggiunta di carte di credito o di debito da un account iTunes Store ad Apple Pay

L'utente potrebbe dover inserire di nuovo la password del proprio ID Apple per utilizzare una carta di credito o di debito registrata in iTunes. Il numero della carta viene recuperato da iTunes, quindi ha inizio il processo di verifica. Se la carta è idonea per Apple Pay, il dispositivo scaricherà e visualizzerà i termini e le condizioni, quindi invierà l'ID dei termini e il codice di sicurezza della carta al processo "Collega e inserisci". Potrebbero essere effettuate ulteriori verifiche per le carte registrate con gli account iTunes.

Aggiungere carte di credito o di debito dall'app dell'emittente

Quando l'app è registrata per l'utilizzo con Apple Pay, vengono stabilite delle chiavi per l'app e per il server dell'emittente. Tali chiavi vengono utilizzate per codificare le informazioni della carta che vengono inviate all'emittente. In questo modo si impedisce che tali informazioni vengano lette dal dispositivo iOS. Il processo di inserimento è simile a quello utilizzato per aggiungere manualmente le carte, descritto precedentemente, con l'unica eccezione che al posto del CVV vengono impiegate delle password utilizzabili una sola volta.

Verifica aggiuntiva

L'emittente può decidere se una carta di credito o di debito richiede ulteriori verifiche. A seconda di quanto predisposto dall'emittente della carta, l'utente potrebbe avere la possibilità di scegliere fra varie opzioni di verifica aggiuntive, per esempio un messaggio di testo, un'e-mail, una telefonata al servizio clienti o un'azione da eseguire in un'app di terze parti per completare la procedura. Per i messaggi di testo e le e-mail, l'utente selezionerà le informazioni di contatto fra i dati in possesso dell'emittente. Riceverà quindi un codice che dovrà essere inserito in Wallet, Impostazioni o nell'app Watch. Per il servizio clienti o per la verifica tramite app, l'emittente adotta il proprio processo di comunicazione.

Autorizzazione dei pagamenti

Sui dispositivi che dispongono di Secure Enclave, i pagamenti saranno consentiti solo dopo che Secure Enclave li avrà autorizzati. Su iPhone o iPad questo processo implica la conferma che l'utente si sia autenticato mediante Touch ID o Face ID o inserendo il codice del dispositivo. Touch ID o Face ID sono i metodi di default, se disponibili, ma al loro posto è possibile utilizzare in qualsiasi momento il codice. L'autenticazione con codice viene proposta automaticamente dopo tre tentativi non riusciti di riconoscimento dell'impronta digitale o due tentativi non riusciti di riconoscimento facciale e diventa obbligatoria dopo cinque tentativi non riusciti. Il codice è richiesto anche quando Touch ID o Face ID non sono configurati o non sono abilitati per Apple Pay. Per effettuare un pagamento su Apple Watch, il dispositivo dev'essere sbloccato con il codice e l'utente deve premere due volte il tasto laterale.

La comunicazione tra Secure Enclave e Secure Element avviene su un'interfaccia seriale, con Secure Element connesso al controller NFC che a sua volta è connesso al processore per le applicazioni. Anche se non sono connessi direttamente, Secure Enclave e Secure Element possono comunicare in maniera sicura utilizzando una chiave di abbinamento condivisa che viene fornita durante il processo di fabbricazione. La codifica e l'autenticazione delle comunicazioni si basano su AES, con nonce di codifica utilizzati da entrambe le parti come protezione contro i replay attack. La chiave di abbinamento è generata all'interno di Secure Enclave a partire dalla sua chiave UID e dall'identificatore univoco di Secure Element. In fabbrica, la chiave di abbinamento viene quindi trasferita da Secure Enclave a un **modulo di sicurezza hardware (Hardware security module, HSM)** che dispone del materiale necessario per inserirla in Secure Element.

Quando l'utente autorizza una transazione, Secure Enclave invia i dati firmati relativi al tipo di autenticazione e i dettagli sul tipo di transazione (contactless o all'interno di app) a Secure Element, legandoli a un valore Authorization Random (AR). Il valore AR è generato in Secure Element quando l'utente fornisce per la prima volta una carta di credito e persiste finché la funzionalità Apple Pay è attiva, protetto dalla codifica e dal meccanismo anti-rollback di Secure Enclave. Viene trasmesso in maniera protetta a Secure Element tramite la chiave di abbinamento. Alla ricezione di un nuovo valore AR, Secure Element contrassegna ogni carta aggiunta in precedenza come eliminata.

Le carte di credito, di debito e prepagate aggiunte a Secure Element possono essere utilizzate solo se Secure Element riceve un'autorizzazione che contiene la stessa chiave di abbinamento e lo stesso valore AR indicati in fase di aggiunta della carta. In questo modo iOS può comunicare a Secure Enclave di rendere le carte inutilizzabili contrassegnando la sua copia del valore AR come non valida nei seguenti scenari:

- Quando il codice è disattivato.
- Quando l'utente esce da iCloud.
- Quando l'utente seleziona “Inizializza contenuto e impostazioni”.
- Quando il dispositivo viene ripristinato dalla modalità di recupero.

Con Apple Watch, le carte sono contrassegnate come non valide:

- Quando il codice dell'orologio è disattivato.
- Quando viene annullato l'abbinamento dell'orologio con iPhone.

Utilizzando la chiave di abbinamento e la sua copia del valore AR attuale, Secure Element verifica l'autorizzazione ricevuta da Secure Enclave prima di abilitare l'applet di pagamento per una transazione contactless. Questo processo viene utilizzato anche per recuperare i dati di pagamento codificati dall'applet di pagamento per le transazioni all'interno delle app.

Codice di sicurezza dinamico specifico per ogni transazione

Le transazioni di pagamento originate dagli applet di pagamento includono un crittogramma di pagamento e un numero di account del dispositivo. Tale crittogramma è un codice valido per un solo uso che viene calcolato utilizzando un contatore che aumenta con ogni nuova transazione, nonché con una chiave inserita nell'applet di pagamento durante la personalizzazione e nota al circuito di pagamento e/o all'emittente. A seconda dello schema di pagamento, per il calcolo possono essere utilizzati anche altri dati, tra cui:

- Un numero imprevedibile del terminale nel caso di una transazione NFC.
- Un nonce del server di Apple Pay nel caso di transazioni all'interno delle app.

I codici di sicurezza vengono forniti al circuito di pagamento e all'emittente in modo da consentire la verifica di ogni transazione. La lunghezza dei codici può variare in base al tipo di transazione in atto.

Pagamento con carte di credito e di debito nei negozi

Se iPhone è acceso e rileva un campo NFC, presenterà all'utente la carta richiesta (se per la carta è attivata la selezione automatica) oppure la carta di default, che viene gestita in Impostazioni. L'utente può anche aprire l'app Wallet e scegliere una carta oppure, quando il dispositivo è bloccato:

- Fare doppio clic sul tasto Home sui dispositivi con Touch ID.
- Fare doppio clic sul tasto laterale sui dispositivi con Face ID.

L'utente dovrà quindi autenticarsi utilizzando Touch ID, Face ID o il proprio codice prima che le informazioni di pagamento vengano trasmesse. Quando Apple Watch è sbloccato, premendo due volte il tasto laterale si attiva la carta di default per il pagamento. Senza l'autenticazione da parte dell'utente non viene inviata alcuna informazione di pagamento.

Una volta completata l'autenticazione, per elaborare il pagamento vengono utilizzati il numero di account del dispositivo e un codice di sicurezza dinamico specifico per la transazione. Né Apple né il dispositivo invieranno al venditore i numeri completi della carta di credito o di debito. Apple potrebbe ricevere informazioni anonime, per esempio ora e posizione approssimative della transazione, che serviranno a migliorare Apple Pay e altri prodotti e servizi Apple.

Pagamento con carte di credito e di debito all'interno delle app

Apple Pay può essere utilizzato anche per effettuare pagamenti all'interno delle app di iOS e di Apple Watch. Quando gli utenti pagano con Apple Pay all'interno delle app, Apple riceve le informazioni codificate sulla transazione e provvede a codificarle nuovamente con una chiave specifica per lo sviluppatore o il venditore prima di trasmettergliele. Apple Pay conserva informazioni anonime sulla transazione, come l'importo approssimativo. Tali informazioni non permettono di risalire all'utente e non includono mai l'oggetto dell'acquisto.

Quando un'app avvia una transazione di pagamento Apple Pay, i server Apple Pay ricevono la transazione codificata dal dispositivo prima che questa arrivi al venditore. I server Apple Pay codificano nuovamente la transazione con una chiave specifica per il venditore prima di trasmetterla a quest'ultimo.

Quando un'app richiede un pagamento, invoca un'API per determinare se il dispositivo supporta Apple Pay e se l'utente ha carte di credito o di debito che possono essere utilizzate su un circuito di pagamento accettato dal venditore. L'app richiede le informazioni necessarie per elaborare e completare la transazione, come ad esempio l'indirizzo di fatturazione e spedizione e i dati di contatto. Quindi l'app chiede a iOS di mostrare la schermata di Apple Pay, la quale richiede informazioni per l'app e altre informazioni necessarie, come ad esempio la carta da utilizzare.

A questo punto vengono fornite all'app le informazioni relative a città, stato e CAP per calcolare le spese di spedizione finali. Il set completo di informazioni viene trasmesso all'app solo quando l'utente autorizza il pagamento con Touch ID, Face ID o con il codice del dispositivo. Una volta autorizzato il pagamento, le informazioni incluse nella schermata di Apple Pay saranno trasferite al venditore.

Quando l'utente autorizza il pagamento, viene inviata una richiesta ai server Apple Pay per ottenere un nonce di codifica, che è simile al valore restituito dal terminale NFC durante le transazioni in negozio. Il nonce viene trasmesso a Secure Element insieme ad altri dati sulla transazione, così da generare una credenziale di pagamento che sarà codificata con una chiave Apple. Quando la credenziale di pagamento codificata lascia Secure Element, viene inoltrata ai server Apple Pay, che la decodificano e confrontano il nonce al suo interno con il nonce originariamente inviato dai server di Apple Pay; la credenziale viene quindi codificata nuovamente con la chiave associata all'ID venditore. A questo punto viene restituita al dispositivo, che la trasferisce all'app attraverso l'API. L'app comunica quindi la credenziale al sistema del venditore per l'elaborazione. Il venditore potrà decodificare la credenziale di pagamento con la propria chiave privata. Unitamente alla firma ricevuta dai server Apple, ciò permette al venditore di verificare che la transazione non fosse destinata ad altri.

Le API richiedono un'autorizzazione che specifichi gli ID venditore supportati. L'app può anche includere dati aggiuntivi da inviare a Secure Element per la firma, come ad esempio un numero d'ordine o l'identità del cliente, così da garantire che la transazione non possa essere dirottata verso un cliente diverso. Questo aspetto è gestito dallo sviluppatore dell'app, che può specificare i valori applicationData sulla richiesta PKPaymentRequest. Un hash di questi dati viene incluso nelle informazioni codificate del pagamento. Il venditore sarà quindi responsabile di verificare che il proprio hash applicationData corrisponda a quanto contenuto nei dati del pagamento.

Pagamento con carte di credito e di debito sul web

Apple Pay può essere utilizzato per effettuare pagamenti sui siti web con i dispositivi iOS, Apple Watch e il Mac. È anche possibile iniziare una transazione di Apple Pay sul Mac e completarla su un iPhone o Apple Watch che utilizza lo stesso account di iCloud ed è abilitato ad effettuare acquisti con Apple Pay.

Apple Pay sul web richiede a tutti i siti web che partecipano di registrarsi con Apple. I server di Apple realizzano la convalida del nome di dominio e rilasciano un certificato cliente TLS. Per potere essere compatibili con Apple Pay, i siti web devono offrire i propri contenuti via HTTPS. Per ogni transazione di pagamento, i siti web devono ottenere una sessione di vendita sicura e unica con un server di Apple tramite il certificato client TLS rilasciato da Apple. I dati della sessione di vendita sono firmati da Apple. Dopo che è stata verificata la firma di una sessione di vendita, il sito web potrebbe inviare una richiesta per sapere se l'utente ha un dispositivo compatibile con Apple Pay e se dispone di una carta di credito, debito o prepagata attivata su tale dispositivo. Non viene condiviso nessun altro dato. Se l'utente non desidera condividere queste informazioni, può disabilitare le richieste di Apple Pay nelle impostazioni relative alla privacy di Safari, sia su iOS che su macOS.

Una volta convalidata la sessione di vendita, le misure di sicurezza e privacy sono le stesse che vengono adottate quando un utente effettua un pagamento dall'interno di un'app.

Nel caso di passaggio da Mac a iPhone o Apple Watch, Apple Pay utilizza il protocollo del servizio di identificazione Apple (IDS) con codifica end-to-end per trasmettere le informazioni relative al pagamento dal Mac dell'utente al dispositivo. IDS utilizza le chiavi del dispositivo dell'utente per la codifica, in modo che nessun altro dispositivo sia in grado di decodificare tali informazioni e che le chiavi non siano disponibili per Apple. Il rilevamento del dispositivo per il passaggio da Mac a un dispositivo iOS durante una transazione di Apple Pay contiene il tipo e l'identificatore unico delle carte di credito dell'utente, oltre alcuni metadati. Il numero di conto associato alla carta dell'utente specifico del dispositivo non viene condiviso e rimane archiviato in modo sicuro su iPhone o Apple Watch dell'utente. Apple trasferisce in modo sicuro tramite il portachiavi iCloud anche gli indirizzi di contatto, fatturazione e spedizione dell'utente usati di recente.

Una volta che l'utente ha autorizzato il pagamento tramite Touch ID, Face ID, il codice oppure premendo due volte il tasto laterale di Apple Watch, viene generato un token di pagamento codificato in modo univoco per ogni certificato di vendita del sito web, che viene trasmesso in modo sicuro da iPhone o Apple Watch al Mac dell'utente e viene quindi consegnato al sito web del venditore.

Il pagamento può essere richiesto e completato unicamente da dispositivi tra loro vicini. La vicinanza è determinata mediante segnali Bluetooth Low Energy.

Biglietti contactless

Wallet supporta il protocollo VAS (Value Added Service) per la trasmissione dei dati dai biglietti supportati ai terminali NFC compatibili. Il protocollo VAS può essere implementato sui terminali contactless e utilizza NFC per comunicare con i dispositivi Apple supportati. Il protocollo VAS funziona entro una breve distanza e può essere utilizzato per presentare biglietti contactless in modo indipendente o come parte di una transazione di Apple Pay.

Quando il dispositivo viene avvicinato al terminale NFC, quest'ultimo avvia la ricezione delle informazioni del biglietto inviando una richiesta di biglietto. Se un utente dispone di un biglietto con l'identificatore del venditore, gli viene richiesto di autorizzarne l'utilizzo tramite Touch ID, Face ID o il codice. Le informazioni del biglietto, la data e l'ora e una chiave casuale ECDH P-256 utilizzabile una sola volta vengono usate insieme alla chiave pubblica del rivenditore per generare una chiave di codifica per i dati del biglietto, che vengono poi inviati al terminale.

Gli utenti possono selezionare un biglietto e autorizzarlo tramite Touch ID, Face ID o il codice anche prima di presentarlo al terminale NFC del venditore.

Apple Pay Cash

In iOS 11.2 o versioni successive e watchOS 4.2 o versioni successive, Apple Pay può essere utilizzato su iPhone, iPad o Apple Watch per inviare, ricevere e richiedere denaro da altri utenti. Il denaro ricevuto da un utente viene aggiunto a un conto Apple Pay Cash accessibile tramite Wallet o da Impostazioni > Wallet e Apple Pay su qualsiasi dispositivo idoneo su cui l'utente abbia effettuato l'accesso con il proprio ID Apple.

Per utilizzare i pagamenti da persona a persona e Apple Pay Cash, l'utente deve aver effettuato l'accesso al proprio account di iCloud su un dispositivo compatibile con il servizio e deve aver configurato l'autenticazione a due fattori sull'account di iCloud.

Quando viene configurato Apple Pay Cash, è possibile che vengano condivise le stesse informazioni necessarie all'aggiunta di carte di credito o di debito con il nostro partner bancario Green Dot Bank e con Apple Payments Inc., una società sussidiaria interamente partecipata creata per proteggere la privacy archiviando ed elaborando le informazioni separatamente dal resto di Apple e senza che vengano divulgate al resto di Apple. Tali informazioni vengono utilizzate solo per la risoluzione di problemi, per proteggere dai tentativi di frode e a scopo normativo.

Le richieste e i trasferimenti tra gli utenti vengono avviate all'interno dell'app Messaggi o chiedendo a Siri. Quando un utente tenta di inviare denaro, iMessage mostra la finestra di Apple Pay. Il saldo presente in Apple Pay Cash viene sempre utilizzato per primo. Se necessario, i fondi aggiuntivi vengono prelevati da una seconda carta di credito o di debito che l'utente ha aggiunto a Wallet.

La carta Apple Pay Cash in Wallet può essere utilizzata con Apple Pay per effettuare pagamenti in negozi, app e sul web. Il denaro presente sul conto di Apple Pay Cash può anche essere trasferito su un conto bancario. Oltre a ricevere denaro da un altro utente, è anche possibile aggiungere denaro al conto di Apple Pay Cash da una carta di debito o prepagata in Wallet.

Una volta completata una transazione, Apple Payments Inc. ne archivia i dati, che può utilizzare per la risoluzione dei problemi, per proteggere dai tentativi di frode e a scopo normativo. Il resto di Apple non è a conoscenza del destinatario o del mittente del denaro né è a conoscenza dei luoghi in cui l'utente ha effettuato acquisti tramite la carta Apple Pay Cash.

Quando l'utente invia denaro con Apple Pay, aggiunge denaro a un conto di Apple Pay Cash o trasferisce denaro su un conto bancario, viene effettuata una chiamata ai server di Apple Pay per ottenere un nonce di codifica, simile al valore restituito per Apple Pay all'interno delle app. Il nonce viene trasmesso a Secure Element insieme ad altri dati sulla transazione, così da generare una firma per il pagamento. Quando la firma del pagamento esce da Secure Element, viene trasmessa ai server di Apple Pay. L'autenticazione, l'integrità e la correttezza della transazione sono verificate dai server di Apple Pay tramite la firma del pagamento e il nonce. Quindi, il trasferimento di denaro viene avviato e l'utente riceve una notifica di transazione completata.

Se la transazione coinvolge una carta di credito o di debito per aggiungere denaro a Apple Pay Cash, inviare denaro a un altro utente o fornire denaro aggiuntivo se il saldo di Apple Pay Cash è insufficiente, viene prodotta anche una credenziale di pagamento codificata che viene inviata ai server di Apple Pay, come quella utilizzata per Apple Pay all'interno delle app.

Se il saldo del conto di Apple Pay Cash supera una certa cifra o se viene rilevata un'attività insolita, all'utente verrà richiesto di verificare la propria identità. Le informazioni fornite per verificare l'identità dell'utente, come il codice fiscale o le risposte a determinate domande (ad esempio, confermare il nome della via in cui hai vissuto in precedenza) vengono trasmesse in maniera sicura al partner di Apple e codificate tramite la rispettiva chiave. Apple non può decodificare tali dati.

Carte dei mezzi pubblici

In Cina e Giappone, gli utenti possono aggiungere carte dei mezzi pubblici supportate in Wallet sui modelli supportati di iPhone e Apple Watch. Possono farlo trasferendo il valore e il titolo di viaggio da una carta fisica nella rappresentazione digitale in Wallet o inserendo una nuova carta dei mezzi pubblici in Wallet dall'app dell'emittente della carta. Una volta che le carte sono state aggiunte in Wallet, gli utenti possono utilizzare i mezzi pubblici semplicemente avvicinando iPhone o Apple Watch all'apposito lettore. In Giappone, la carta Suica può essere utilizzata anche per effettuare pagamenti.

Le carte dei mezzi pubblici aggiunte sono associate all'account di iCloud dell'utente. Se l'utente aggiunge più di una carta a Wallet, Apple o la compagnia di trasporti potrebbero essere in grado di collegare le informazioni personali dell'utente e le relative informazioni dell'account tra le varie carte. Ad esempio, le carte MySuica possono essere collegate a carte Suica anonime. Le carte e le transazioni relative ai mezzi di trasporto sono protette da un insieme di chiavi di codifica gerarchiche.

Durante il processo di trasferimento del saldo da una carta fisica a Wallet, all'utente viene richiesto di inserire le cifre identificative del numero di serie della carta. Agli utenti potrebbe anche essere richiesto di fornire informazioni personali per dimostrare di essere i possessori della carta. Ad esempio, se la carta è una MySuica o una carta Suica contenente un titolo di viaggio, l'utente dovrà inserire anche la propria data di nascita. Durante il trasferimento dei biglietti da iPhone ad Apple Watch, entrambi i dispositivi devono essere in linea.

Il saldo può essere ricaricato con fondi da carte di credito o prepagate tramite Wallet o dall'app dell'emittente della carta dei mezzi pubblici. Le informazioni di sicurezza sul caricamento del saldo quando si utilizza Apple Pay sono descritte nella sezione "Pagamento con carte di credito e di debito all'interno delle app" di questo documento.

La procedura di inserimento della carta dei mezzi pubblici dall'app dell'emittente è descritto nella sezione "Aggiunta di carte di credito o di debito dall'app dell'emittente" di questo documento.

L'emittente della carta dispone delle chiavi di codifica necessarie all'autenticazione della carta fisica e alla verifica dei dati inseriti dall'utente. Una volta verificati, il sistema può creare un numero di account per il dispositivo per Secure Element e attivare il biglietto appena aggiunto su Wallet con il saldo trasferito. In Giappone, una volta completato l'inserimento della carta fisica, la carta fisica Suica viene disabilitata.

Alla fine di entrambi i processi di inserimento, il saldo della carta viene codificato e archiviato in un apposito applet in Secure Element. La compagnia di trasporti dispone delle chiavi per eseguire le operazioni di codifica sui dati della carta per le transizioni con il saldo.

Di default, gli utenti possono sfruttare l'opzione Express Transit, che consente loro di pagare ed effettuare corse senza che venga richiesto l'uso di Touch ID, Face ID o del codice. Informazioni come le stazioni visitate di recente, la cronologia delle transazioni e i biglietti aggiuntivi sono accessibili da parte di qualsiasi lettore di carte contactless vicino che abbia l'opzione Express Mode abilitata. Gli utenti possono abilitare la richiesta di autorizzazione tramite Touch ID, Face ID o codice nelle impostazioni "Wallet e Apple Pay", disabilitando la funzionalità Express Transit.

Come per le altre carte di Apple Pay, per sospendere o rimuovere le carte dei mezzi pubblici, gli utenti possono:

- Inizializzare il dispositivo da remoto con "Trova il mio iPhone".
- Abilitare la modalità smarrito con "Trova il mio iPhone".
- Inizializzare il dispositivo da remoto tramite una soluzione MDM.
- Rimuovere tutte le carte dalla pagina dell'account dell'ID Apple.
- Rimuovere tutte le carte da iCloud.com.
- Rimuovere tutte le carte da Wallet.
- Rimuovere la carta dall'app dell'emittente.

I server di Apple Pay invieranno una richiesta alla compagnia di trasporti per sospendere o disabilitare tali carte. Per la carte Suica, se il dispositivo dell'utente non è in linea durante un tentativo di inizializzazione, le carte Suica potrebbero ancora essere utilizzabili presso alcuni terminali fino alle ore 12:01 JST del giorno successivo. Se il dispositivo dell'utente non è in linea, le carte dei mezzi pubblici in Cina continuano a essere disponibili per l'utilizzo.

Se gli utenti rimuovono le proprie carte dei mezzi pubblici, il saldo può essere recuperato aggiungendole di nuovo a un dispositivo con lo stesso ID Apple.

Tessere identificative studente

In iOS 12, gli studenti, i docenti e il personale degli istituti didattici partecipanti possono aggiungere la propria tessera identificativa a Wallet per accedere alle strutture e pagare presso le attività che accettano la tessera.

Gli utenti aggiungono la tessera identificativa a Wallet attraverso un'app fornita dall'emittente della stessa o dalla scuola partecipante. Il procedimento tecnico impiegato è lo stesso descritto precedentemente nella sezione “Aggiunta di carte di credito o di debito dall'app dell'emittente” di questo documento. Inoltre, le app dell'emittente devono supportare l'autenticazione a due fattori sugli account che controllano l'accesso alle tessere identificative. Ciascuna tessera può essere configurata contemporaneamente su due dispositivi Apple supportati sui cui è stato effettuato l'accesso con lo stesso ID Apple.

Quando viene aggiunta una tessera identificativa studente a Wallet, di default viene attivata la modalità rapida. Le tessere identificative studente in modalità rapida interagiscono con i terminali riceventi senza l'autenticazione tramite Touch ID, Face ID o codice. L'utente può toccare il pulsante Altro sulla tessera in Wallet e disattivare la modalità rapida per disabilitare questa funzionalità. Per riabilitare la modalità rapida è richiesto Touch ID, Face ID o il codice.

Per disabilitare o rimuovere le tessere identificative studente, gli utenti possono:

- Inizializzare il dispositivo da remoto con “Trova il mio iPhone”.
- Abilitare la modalità smarrito con “Trova il mio iPhone”.
- Inizializzare il dispositivo da remoto tramite una soluzione MDM.
- Rimuovere tutte le carte dalla pagina dell'account dell'ID Apple.
- Rimuovere tutte le carte da iCloud.com.
- Rimuovere tutte le carte da Wallet.
- Rimuovere la tessera dall'app dell'emittente.

Sospendere, rimuovere e cancellare le carte

Gli utenti possono interrompere l'uso di Apple Pay su iPhone, iPad e Apple Watch attivando la modalità smarrito sul dispositivo con “Trova il mio iPhone”. Inoltre, hanno la possibilità di rimuovere e cancellare le proprie carte da Apple Pay utilizzando “Trova il mio iPhone”, iCloud.com o direttamente tramite Wallet sui dispositivi. Su Apple Watch è possibile rimuovere le carte utilizzando le impostazioni di iCloud o l'app Apple Watch su iPhone, oppure direttamente l'orologio. L'emittente o il relativo circuito sospenderà o rimuoverà l'abilitazione ai pagamenti con carte da Apple Pay anche se il dispositivo non è in linea e non è connesso a una rete Wi-Fi o cellulare. Gli utenti possono inoltre chiamare il proprio emittente per chiedere la sospensione o la rimozione delle carte da Apple Pay.

Inoltre, quando un utente inizializza l'intero dispositivo tramite “Inizializza contenuto e impostazioni”, tramite “Trova il mio iPhone” o ripristinandolo in modalità di recupero, iOS farà sì che Secure Element contrassegni tutte le carte come eliminate. Le carte risulteranno così inutilizzabili con effetto immediato fino a quando non sarà possibile contattare i server Apple Pay per cancellarle completamente da Secure Element. In modo indipendente, Secure Enclave contrassegna il valore AR come non valido al fine di impedire ulteriori autorizzazioni di pagamento per le carte precedentemente registrate. Quando è in linea, il dispositivo tenta di contattare i server Apple Pay per assicurarsi che tutte le carte in Secure Element vengano cancellate.

Servizi Internet

Creazione di password sicure per gli ID Apple
Gli ID Apple vengono utilizzati per accedere a una varietà di servizi, tra cui iCloud, FaceTime e iMessage. Per aiutare gli utenti a creare password sicure, tutti i nuovi account devono utilizzare password con le seguenti caratteristiche:

- Almeno otto caratteri.
- Almeno una lettera.
- Almeno una lettera maiuscola.
- Almeno un numero.
- Non più di tre caratteri identici consecutivi.
- Diversa dal nome account.

Per aiutare gli utenti a usare i propri dispositivi in modo ancora più utile e produttivo, Apple ha creato un robusto set di servizi come iMessage, FaceTime, Suggerimenti Siri, il backup iCloud e il portachiavi iCloud.

Tali servizi Internet sono stati sviluppati con gli stessi obiettivi di sicurezza promossi da iOS a ogni livello della piattaforma, per esempio: gestione sicura dei dati, sia in locale sul dispositivo che in transito sulle reti wireless; protezione delle informazioni personali degli utenti; protezione dagli accessi dannosi o non autorizzati a informazioni e servizi. Ogni servizio utilizza una propria potente architettura di sicurezza senza compromettere la complessiva facilità d'uso di iOS.

ID Apple

L'ID Apple è l'account utilizzato per accedere a servizi Apple come iCloud, iMessage, FaceTime, iTunes Store, Apple Books, App Store e altro ancora. È importante che gli utenti tengano al sicuro i propri ID Apple, così da evitare l'accesso non autorizzato ai loro account. Per una maggiore protezione, Apple richiede di impostare password difficili da indovinare, di lunghezza non inferiore a otto caratteri, formate da lettere e numeri, che non contengano più di tre caratteri identici consecutivi e che non siano password comunemente usate. Gli utenti sono incoraggiati ad andare oltre queste linee guida, aggiungendo altri caratteri e segni di punteggiatura per rendere le password ancora più efficaci. Apple chiede inoltre agli utenti di configurare tre domande di sicurezza che potranno essere utilizzate come strumento ausiliare per la verifica dell'identità del proprietario quando l'utente vuole apportare delle modifiche alle informazioni contenute nel proprio account o quando desidera reimpostare una password dimenticata.

Inoltre, Apple invia e-mail e notifiche push agli utenti quando vengono effettuati cambiamenti importanti ai loro account, per esempio la modifica di una password o delle informazioni di fatturazione oppure se l'ID Apple è stato utilizzato per accedere a un servizio su un nuovo dispositivo. Gli utenti sono invitati a cambiare immediatamente la password dell'ID Apple qualora non ricordino di avere effettuato la modifica in questione.

Inoltre, Apple fa uso di una gamma di politiche e procedure volte a proteggere gli account utente. Tra queste, vi è la limitazione del numero di tentativi errati di accesso o di reimpostazione della password, il controllo attivo anti-frode, per aiutare nell'identificazione degli attacchi nel momento in cui si verificano e revisioni periodiche delle proprie politiche, che consentono ad Apple di adattarsi a eventuali informazioni che possono riguardare la sicurezza degli utenti.

Autenticazione a due fattori

Per aiutare gli utenti a proteggere ancora di più i propri account, Apple offre l'*autenticazione a due fattori*, un ulteriore livello di sicurezza per gli ID Apple. È pensata per garantire che l'accesso all'account possa avvenire unicamente da parte del proprietario dell'account, anche nel caso in cui qualcun altro sia a conoscenza della password.

Con l'autenticazione a due fattori, l'accesso a un account utente può avvenire solo su dispositivi autorizzati, come iPhone, iPad o il Mac dell'utente. Per effettuare l'accesso per la prima volta su un nuovo dispositivo, occorrono due dati: la password dell'ID Apple e un codice di verifica a sei cifre che viene visualizzato automaticamente sui dispositivi autorizzati dell'utente oppure inviato a un numero di telefono autorizzato. Inserendo il codice, l'utente dimostra di voler autorizzare il nuovo dispositivo e di considerare sicuro l'accesso. Poiché la sola password non è più sufficiente a garantire l'accesso a un account utente, l'autenticazione a due fattori rappresenta un miglioramento della sicurezza dell'ID Apple e di tutte le informazioni personali archiviate presso Apple. È integrata in iOS, macOS, tvOS, watchOS e nei sistemi di autenticazione utilizzati da siti web di Apple.

Per ulteriori informazioni sull'autenticazione a due fattori, consulta: https://support.apple.com/HT204915

Verifica in due passaggi

Dal 2013, inoltre, Apple offre un metodo di sicurezza simile chiamato "*Verifica in due passaggi*". Quando la verifica in due passaggi è abilitata, l'identità dell'utente deve essere verificata tramite un codice temporaneo inviato a uno dei suoi dispositivi autorizzati; una volta avvenuta tale verifica dell'identità, l'utente potrà modificare i dati dell'ID Apple, accedere a iCloud, iMessage, FaceTime o Game Center o effettuare acquisti su iTunes Store, Apple Books o App Store da un nuovo dispositivo. Inoltre, agli utenti viene fornita una chiave di recupero di 14 caratteri, da conservare in un luogo sicuro e da utilizzare nel caso in cui dimentichino la password o non riescano ad accedere ai dispositivi autorizzati. Sebbene la maggioranza degli utenti sia incoraggiata a utilizzare l'autenticazione a due fattori, ci sono comunque alcune situazioni in cui è preferibile utilizzare la verifica in due passaggi.

Per ulteriori informazioni sulla verifica in due passaggi dell'ID Apple, consulta: https://support.apple.com/ht5570

ID Apple gestiti

Gli ID Apple gestiti funzionano in modo simile a un ID Apple, ma sono di proprietà di un ente educativo e controllati da tale centro, che può reimpostare le password, limitare gli acquisti e l'uso di app per la comunicazione, come FaceTime e Messaggi, e configurare dei permessi, diversi in base al ruolo, per il personale, per docenti e per studenti.

Alcuni servizi di Apple sono disabilitati per gli ID Apple gestiti, come ad esempio: Apple Pay, Portachiavi iCloud, HomeKit e "Trova il mio iPhone".

Per ulteriori informazioni sugli ID Apple gestiti, consulta: https://help.apple.com/schoolmanager/#/tes78b477c81

Controllo degli ID Apple gestiti

Gli ID Apple gestiti supportano inoltre la possibilità di essere controllati, consentendo così agli enti educativi di soddisfare le norme legali e relative alla privacy. Gli account di amministratore, manager o docente possono avere privilegi di controllo su ID Apple specifici. Un utente può controllare unicamente account di livello inferiore nella gerarchia dell'ente; ossia: i docenti possono controllare gli studenti; i manager possono controllare i docenti e gli studenti; gli amministratori possono controllare manager, docenti e studenti.

Quando, tramite Apple School Manager, vengono richieste delle credenziali per il controllo, viene creato un account speciale che ha accesso solo all'ID Apple gestito per cui è stato richiesto il controllo. I permessi per il controllo scadono dopo sette giorni. Durante tale periodo, chi sta effettuando il controllo può leggere e modificare i contenuti dell'utente controllato archiviati su iCloud o in app con CloudKit abilitato. Tutte le richieste di accesso con privilegi di controllo vengono registrate in Apple School Manager. I log mostrano il nome di chi ha inoltrato la richiesta, l'ID Apple gestito per cui è stata effettuata la richiesta di controllo, l'ora della richiesta e se il controllo è stato effettivamente realizzato.

Per ulteriori informazioni sul controllo degli ID Apple gestiti, consulta: https://help.apple.com/schoolmanager/#/tesd8fcbdd99

ID Apple gestiti e dispositivi personali

Gli ID Apple gestiti possono essere utilizzati anche sui dispositivi iOS e sui computer Mac personali. Gli studenti accedono a iCloud usando l'ID Apple gestito fornito dall'ente educativo e un'ulteriore password per uso domestico che funge da secondo fattore del processo di autenticazione a due fattori dell'ID Apple. Mentre l'utente usa un ID Apple gestito su un dispositivo personale, il portachiavi iCloud non è disponibile; l'ente educativo potrebbe inoltre limitare l'uso di altre funzionalità come FaceTime o Messaggi. Qualsiasi documento creato degli studenti mentre hanno effettuato l'accesso è soggetto al controllo nella maniera descritta precedentemente in questa sezione.

iMessage

Apple iMessage è un servizio di messaggistica per dispositivi iOS, Apple Watch e computer Mac che supporta testo e allegati come foto, contatti e posizioni. I messaggi compaiono su tutti i dispositivi registrati dell'utente, in modo da poter continuare la conversazione su qualsiasi dispositivo. iMessage fa un uso estensivo del servizio di notifiche Apple Push Notification (APN). Apple non tiene traccia di messaggi o allegati e i loro contenuti sono protetti da una codifica end-to-end in modo che solo il mittente e il destinatario possano accedervi. Apple non può decodificare dati.

Quando l'utente attiva iMessage su un dispositivo, il dispositivo genera due coppie di chiavi da utilizzare con il servizio: una chiave RSA a 1280 bit per la codifica e una chiave ECDSA a 245 bit sulla curva NIST P-256 per la firma. Le chiavi private di entrambe le coppie sono salvate nel portachiavi del dispositivo, mentre le chiavi pubbliche vengono inviate al servizio di identificazione Apple (IDS), dove sono associate al numero di telefono o all'indirizzo e-mail dell'utente, insieme all'indirizzo APN del dispositivo.

Man mano che gli utenti abilitano altri dispositivi per l'utilizzo di iMessage, le loro chiavi pubbliche per la codifica e la firma, gli indirizzi APN e i numeri di telefono associati vengono aggiunti al servizio di directory. Gli utenti possono anche aggiungere altri indirizzi e-mail, che vengono verificati con l'invio di un link di conferma. I numeri di telefono vengono verificati dalla rete e dalla SIM del gestore. Con alcune reti, tale operazione richiede l'utilizzo del servizio SMS (all'utente verrà mostrata una finestra di conferma se il messaggio SMS non è gratuito). La verifica del numero di telefono può essere richiesta per vari servizi di sistema oltre a iMessage, come FaceTime e iCloud. Tutti i dispositivi registrati dell'utente mostrano un messaggio di avviso all'aggiunta di un nuovo dispositivo, numero di telefono o indirizzo e-mail.

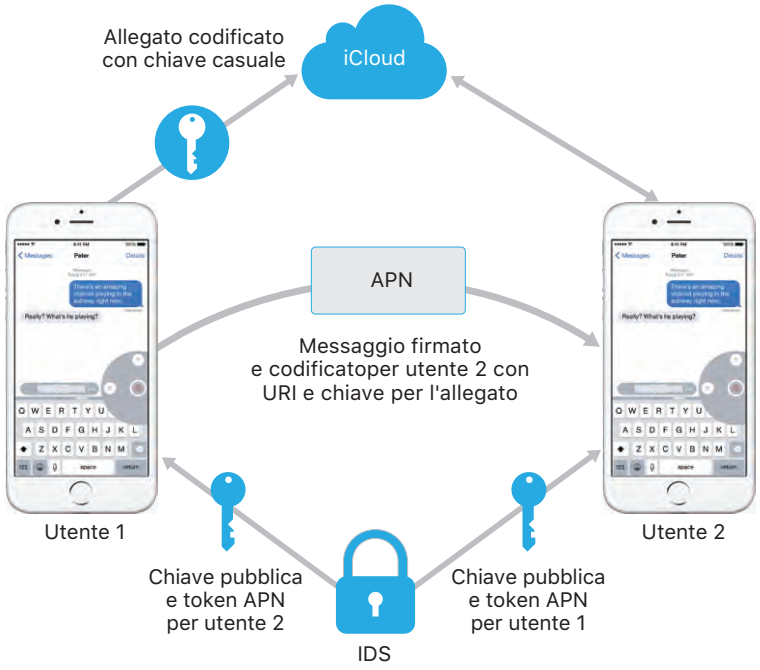
In iOS 12 o versioni successive, i messaggi inviati da indirizzi diversi che sono collegati allo stesso ID Apple, vengono mostrati in un'unica conversazione sui dispositivi che li ricevono. Ciò è facilitato da un identificativo dell'account raccolto dal servizio di identificazione Apple insieme alla chiave pubblica e agli indirizzi APN per gli indirizzi e-mail o i numeri di telefono.

Processo di invio e ricezione dei messaggi con iMessage

Gli utenti avviano una nuova conversazione iMessage inserendo un indirizzo o un nome. Se inseriscono un numero di telefono o un indirizzo e-mail, il dispositivo contatta l'IDS per recuperare le chiavi pubbliche e gli indirizzi APN di tutti i dispositivi associati al destinatario. Se l'utente inserisce un nome, il dispositivo utilizza prima l'app Contatti per ottenere i numeri di telefono e gli indirizzi e-mail associati al nominativo, quindi recupera le chiavi pubbliche e gli indirizzi APN dall'IDS.

Il messaggio in uscita viene codificato individualmente per ciascun dispositivo del destinatario. Le chiavi di codifica RSA pubbliche dei dispositivi riceventi vengono recuperate dall'IDS. Per ogni dispositivo di ricezione, il dispositivo di invio genera un valore a 88 bit casuale e lo utilizza come chiave HMAC-SHA256 per costruire un valore a 40 bit derivato dalla chiave pubblica del mittente e del ricevente, oltre che dal testo. La concatenazione dei valori a 88 e 40 bit crea una chiave a 128 bit, che codifica il messaggio tramite AES in modalità CTR. Il valore a 40 bit è utilizzato dal ricevente per verificare l'integrità del testo decodificato. Questa chiave AES per messaggio è codificata utilizzando RSA-OAEP sulla chiave pubblica del dispositivo ricevente. La combinazione di testo del messaggio codificato e chiave del messaggio codificata viene quindi sottoposta a hashing con SHA-1; a questo punto, l'hash viene firmato con ECDSA utilizzando la chiave privata per la firma del dispositivo mittente. I messaggi risultanti, uno per ciascun dispositivo ricevente e contenenti il testo del messaggio codificato, la chiave del messaggio codificata e la firma digitale del mittente, sono quindi inviati al servizio APN per la consegna. I metadati, come l'indicazione di data e ora e le informazioni per l'instradamento via APN, non sono codificati. La comunicazione con il servizio APN è codificata utilizzando un canale TLS forward-secret.

Il servizio APN può solo inoltrare messaggi di dimensioni fino a 4 KB o 16 KB, a seconda della versione di iOS. Se il messaggio è troppo lungo, o se contiene un allegato come una foto, l'allegato viene codificato utilizzando AES in modalità CTR con una chiave casuale a 256 bit e quindi caricato su iCloud. La chiave AES per l'allegato, il suo **URI (Uniform Resource Identifier)** e l'hash SHA-1 della sua forma codificata vengono quindi inviati al destinatario come contenuti di un iMessage; la riservatezza e l'integrità dei contenuti sono protette tramite la normale codifica di iMessage, come mostrato nel seguente diagramma.



Per le conversazioni di gruppo, questo processo viene ripetuto per ogni destinatario e per ciascuno dei loro dispositivi.

Sul lato del destinatario, ogni dispositivo riceve la propria copia del messaggio dal servizio APN e, se necessario, recupera l'allegato da iCloud. Il numero di telefono o l'indirizzo e-mail del mittente viene confrontato con i contatti del destinatario per poter visualizzare un nome, se possibile.

Come per tutte le notifiche push, il messaggio viene eliminato dal servizio APN una volta consegnato. Tuttavia, a differenza di altre notifiche APN, i messaggi iMessage vengono messi in coda per essere consegnati sui dispositivi non in linea. Attualmente i messaggi restano memorizzati per un massimo di 30 giorni.

Chat con l'azienda

"Chat con l'azienda" è un servizio di messaggistica che consente agli utenti di comunicare con le aziende tramite l'app Messaggi. Solo gli utenti possono avviare la conversazione e l'azienda riceve un identificativo che non rivela alcuna informazione sull'utente. L'azienda non riceve il numero di telefono, l'indirizzo e-mail o le informazioni dell'account di iCloud. Quando avvii una chat con Apple, Apple riceve un ID associato al tuo ID Apple. La volontà di stabilire una comunicazione rimane sotto il controllo degli utenti. Eliminando una conversazione di "Chat con l'azienda", questa viene rimossa dall'app Messaggi dell'utente e l'azienda non potrà inviargli ulteriori messaggi.

I messaggi inviati alle aziende vengono codificati individualmente tra il dispositivo dell'utente e i server di messaggistica di Apple e i server di messaggistica di Apple decodificano i messaggi e li inoltrano all'azienda tramite TLS. Le risposte delle aziende sono similmente inviati tramite TLS ai server di messaggistica di Apple, che ricodificano il messaggio verso il dispositivo dell'utente. Come per iMessage, i messaggi vengono inseriti in una coda per la consegna ai dispositivi non in linea per un periodo massimo di 30 giorni.

FaceTime

FaceTime è il servizio di Apple per chiamate video e audio. In modo simile a iMessage, anche le chiamate FaceTime utilizzano il servizio di notifiche push di Apple per stabilire una connessione iniziale con i dispositivi registrati dell'utente. I contenuti audio/video delle chiamate FaceTime sono protetti da codifica end-to-end, in modo che solo il mittente e il destinatario possano accedervi. Apple non può decodificare dati.

La connessione FaceTime iniziale viene effettuata tramite l'infrastruttura dei server Apple, che fungono da elemento di trasmissione dei pacchetti tra i dispositivi registrati degli utenti. Tramite le notifiche APN e i messaggi STUN (Session Traversal Utilities for NAT) attraverso questa connessione, i dispositivi verificano i propri certificati di identità e stabiliscono un segreto condiviso per ogni sessione. Il segreto condiviso è utilizzato per generare le chiavi di sessione per i canali multimediali trasmessi in streaming tramite il protocollo SRTP Secure Real-time Transport Protocol. I pacchetti SRTP sono codificati tramite AES-256 in Counter Mode e HMAC-SHA1. Dopo la connessione iniziale e la configurazione della sicurezza, FaceTime utilizza i protocolli STUN e ICE (Internet Connectivity Establishment) per stabilire una connessione peer-to-peer tra i dispositivi, se possibile.

Le chiamate FaceTime di gruppo estendono le capacità di FaceTime per supportare fino a 33 partecipanti contemporaneamente. Così come per le chiamate FaceTime singole classiche, le chiamate di gruppo usufruiscono della codifica end-to-end tra i dispositivi dei partecipanti invitati. Mentre gran parte dell'infrastruttura e del design delle chiamate FaceTime singole vengono riutilizzati, le chiamate FaceTime di gruppo sono dotate di un nuovo meccanismo per la definizione delle chiavi che va ad aggiungersi all'autenticazione fornita da IDS. Grazie alla segretezza fornita da questo protocollo, la compromissione del dispositivo di un utente non comporterà la fuga dei contenuti delle chiamate precedenti. Le chiavi della sessione vengono cifrate tramite AES-SIV e distribuite tra i partecipanti tramite una costruzione ECIES con chiavi effimere P-256 ECDH.

Quando un nuovo numero di telefono o indirizzo e-mail viene aggiunto a una chiamata FaceTime di gruppo in corso, i dispositivi attivi stabiliscono nuove chiavi multimediali e non condivideranno mai le chiavi utilizzate con i nuovi dispositivi invitati.

iCloud

iCloud archivia contatti, calendari, foto, documenti e altri file dell'utente mantenendoli aggiornati su tutti i suoi dispositivi, automaticamente. Può essere utilizzato anche da app di terze parti per memorizzare e sincronizzare non solo documenti, ma anche i valori chiave per i dati delle app, come definito dallo sviluppatore. Gli utenti possono configurare iCloud accedendo con un ID Apple e scegliendo quali servizi desiderano utilizzare. Gli amministratori IT hanno la possibilità di disattivare funzionalità di iCloud come "Il mio streaming foto", iCloud Drive e il backup su iCloud servendosi dei profili di configurazione tramite soluzioni MDM. Il servizio non è al corrente di cosa viene archiviato e tratta tutti i file allo stesso modo, ovvero come una raccolta di byte.

Ogni file viene suddiviso in blocchi, quindi codificato da iCloud utilizzando AES-128 e una chiave derivata dai contenuti di ciascun blocco e basata sullo standard SHA-256. Le chiavi e i metadati del file sono archiviati da Apple nell'account iCloud dell'utente. I blocchi codificati del file vengono archiviati, senza alcuna chiave o informazione che identifichi l'utente, utilizzando sia servizi di archiviazione Apple che di terze parti.

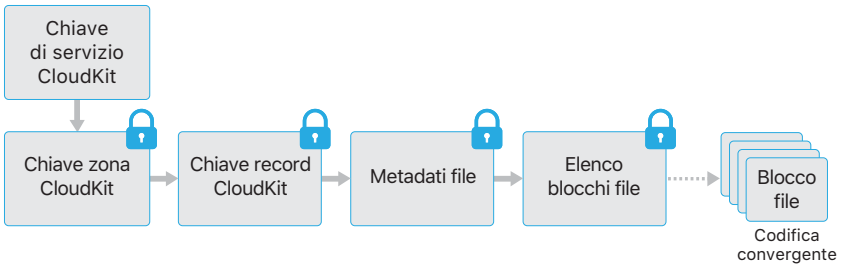
iCloud Drive

iCloud Drive aggiunge chiavi basate sull'account per proteggere i documenti archiviati in iCloud. Come per altri servizi iCloud, i contenuti del file vengono suddivisi in blocchi e codificati, per poi essere archiviati utilizzando servizi di terze parti. Le chiavi dei contenuti del file vengono invece cifrate con chiavi record memorizzate insieme ai metadati di iCloud Drive. A loro volta, le chiavi record sono protette dalla chiave del servizio iCloud Drive dell'utente, che viene quindi archiviata con il suo account iCloud. Per accedere ai metadati dei propri documenti iCloud, gli utenti devono non solo autenticarsi in iCloud, ma anche essere in possesso della chiave del servizio iCloud Drive, che consente di visualizzare le parti protette del relativo spazio di archiviazione.

CloudKit

CloudKit permette agli sviluppatori di app di archiviare dati valore-chiave, dati strutturati e risorse in iCloud. L'accesso a CloudKit viene controllato utilizzando le autorizzazioni delle app. CloudKit supporta database sia pubblici che privati. I database pubblici sono utilizzati da tutte le copie dell'app, solitamente per le risorse generiche, e non sono codificati. I database privati contengono i dati dell'utente.

Come iCloud Drive, anche CloudKit utilizza chiavi basate sull'account per proteggere le informazioni memorizzate nel database privato dell'utente; inoltre, come avviene per altri servizi iCloud, i file sono suddivisi in blocchi, codificati e archiviati utilizzando servizi di terze parti. CloudKit utilizza una gerarchia di chiavi, simile a quella utilizzata per la protezione dati. Le chiavi per file sono cifrate da chiavi record CloudKit che, a loro volta, sono protette da una chiave a livello di zona mantenuta al sicuro dalla chiave del servizio CloudKit dell'utente. La chiave del servizio CloudKit è memorizzata nell'account iCloud dell'utente ed è disponibile solo dopo che questi si è autenticato in iCloud.



Codifica end-to-end di CloudKit

Apple Pay Cash, i dati sanitari, le parole chiave utente, Siri Intelligence ed "Ehi Siri" utilizzano la codifica end-to-end di CloudKit con una chiave di servizio di CloudKit protetta tramite la sincronizzazione del portachiavi iCloud. Tali contenitori CloudKit hanno il root della chiave gerarchica nel portachiavi iCloud, quindi ne condividono le caratteristiche di sicurezza: le chiavi sono disponibili solo per i dispositivi approvati dell'utente e non per Apple o qualsiasi terza parte. Se l'accesso ai dati del portachiavi iCloud viene perso (consulta la sezione "Sicurezza del servizio di deposito" più avanti in questo documento), i dati in CloudKit vengono inizializzati e se sono disponibili dal dispositivo locale autorizzato, vengono ricaricati su CloudKit.

Anche Messaggi su iCloud utilizza la codifica end-to-end di CloudKit con una chiave di servizio di CloudKit protetta con la sincronizzazione del portachiavi iCloud. Se l'utente ha abilitato i backup di iCloud, la chiave di servizio di CloudKit utilizzata per il contenitore di Messaggi su iCloud viene inclusa nel backup su iCloud, per consentire all'utente di recuperare i messaggi anche se ha perso l'accesso al portachiavi iCloud e ai dispositivi autorizzati. Questa chiave di servizio di iCloud viene rinnovata ogni volta che l'utente disattiva il backup su iCloud.

Backup iCloud

iCloud effettua anche il backup quotidiano via Wi-Fi di una serie di informazioni, tra cui impostazioni del dispositivo, dati delle app, foto e video in "Rullino foto", nonché conversazioni nell'app Messaggi. iCloud protegge i contenuti codificandoli quando li trasmette via Internet, archiviandoli in forma codificata e utilizzando token sicuri per l'autenticazione. Il backup su iCloud ha luogo solo quando il dispositivo è bloccato, è collegato a una fonte di alimentazione e ha accesso Wi-Fi a Internet. Vista la codifica utilizzata in iOS, il sistema è progettato per mantenere i dati al sicuro pur consentendo backup incrementali e operazioni di ripristino senza interventi da parte dell'utente.

Di seguito sono riportati i dati inclusi nei backup di iCloud:

- Dati di musica, film, programmi TV, app e libri acquistati. Il backup di iCloud di un utente include le informazioni relative ai contenuti acquistati presenti sul dispositivo iOS dell'utente, ma non i contenuti stessi. Quando l'utente effettua il ripristino da un backup di iCloud, i contenuti che aveva acquistato vengono scaricati automaticamente da iTunes Store, Apple Books o App Store. Alcuni tipi di contenuto non vengono scaricati automaticamente in tutti i paesi o in tutte le aree e gli acquisti effettuati in precedenza potrebbero non essere disponibili se sono stati rimborsati o non sono più disponibili sullo store. La cronologia completa degli acquisti è associata all'ID Apple dell'utente.

Opzioni di recupero

Situazione	Opzioni di recupero per l'utente per la codifica end-to-end di CloudKit
Accesso a dispositivo autorizzato	Recupero dati possibile tramite dispositivo autorizzato o recupero del portachiavi iCloud.
Nessun dispositivo autorizzato	Recupero dati possibile solo tramite recupero del portachiavi iCloud.

Situazione	Opzioni di recupero per l'utente per Messaggi su iCloud
Backup di iCloud abilitato e accesso a dispositivo autorizzato	Recupero dati possibile tramite backup di iCloud, accesso a dispositivo autorizzato o recupero del portachiavi iCloud.
Backup di iCloud abilitato e nessun accesso a dispositivo autorizzato	Recupero dati possibile tramite backup di iCloud e recupero del portachiavi iCloud.
Backup di iCloud disabilitato e accesso a dispositivo autorizzato	Recupero dati possibile tramite dispositivo autorizzato o recupero del portachiavi iCloud.
Backup disabilitato e nessun dispositivo autorizzato	Recupero dati possibile solo tramite recupero del portachiavi iCloud.

- Foto e video sul dispositivo iOS di un utente. Se un utente attiva la libreria foto di iCloud sui dispositivi iOS (iOS 8.1 o successivo) o sul Mac (OS X 10.10.3 o versione successiva), le sue foto e i suoi video sono già archiviati su iCloud, quindi non saranno inclusi nel backup di iCloud per quell'utente.
- Contatti, eventi del calendario, promemoria e note.
- Impostazioni del dispositivo.
- Dati delle app.
- La cronologia delle chiamate e le suonerie.
- Schermata Home e organizzazione delle app.
- Configurazione di HomeKit.
- Password della segreteria visiva (richiede la scheda SIM che era in uso durante il backup).
- iMessage, "Chat con l'azienda", messaggi di testo (SMS) e MMS (richiede la scheda SIM che era in uso durante il backup).

Nota: Quando Messaggi su iCloud è abilitato, iMessage, "Chat con l'azienda", i messaggi di testo (SMS) e i messaggi MMS vengono rimossi dal backup di iCloud esistente dell'utente e vengono archiviati invece in un contenitore CloudKit con codifica end-to-end per Messaggi. Il backup di iCloud dell'utente conserva una chiave per tale contenitore. Se in seguito l'utente disabilita il backup su iCloud, la chiave del contenitore viene rinnovata, la nuova chiave è archiviata solo nel portachiavi iCloud (inaccessibile a Apple e da qualsiasi terza parte) e i nuovi dati scritti nel contenitore non possono essere decodificati con la vecchia chiave.

Quando i file vengono creati in classi di protezione dati non accessibili a dispositivo bloccato, le loro chiavi per file sono codificate utilizzando le chiavi di classe provenienti dalla keybag Backup iCloud. I file vengono copiati su iCloud nel loro stato codificato originale. I file nella classe di protezione dati "Nessuna protezione" sono codificati durante il trasferimento.

La keybag Backup iCloud contiene chiavi asimmetriche (Curve25519) per ciascuna classe di protezione dati, utilizzate per codificare le chiavi per file. Per maggiori informazioni sui contenuti della keybag Backup e la keybag Backup iCloud, consulta "Protezione dati del portachiavi" nella sezione "Codifica e protezione dati" di questo documento.

Il set di backup è archiviato nell'account iCloud dell'utente ed è formato da una copia dei file dell'utente e dalla keybag Backup iCloud. La keybag Backup iCloud è protetta da una chiave casuale, anch'essa archiviata insieme al set di backup (la password iCloud dell'utente non viene utilizzata per la codifica, così da non invalidare i backup qualora venisse modificata).

Nonostante venga copiato su iCloud, il database del portachiavi dell'utente resta protetto da una chiave legata all'UID. In questo modo il portachiavi può essere ripristinato solo sul dispositivo su cui è stato generato; questo significa che nessun altro, Apple inclusa, potrà leggere gli elementi del portachiavi dell'utente.

La procedura di ripristino recupera i file copiati nel backup, la keybag Backup iCloud e la chiave della keybag dall'account iCloud dell'utente. La keybag Backup iCloud viene decodificata utilizzando la relativa chiave, quindi si utilizzano le chiavi per file nella keybag per decodificare i file nel set di backup, che vengono scritti ex novo nel file system e quindi nuovamente codificati in base alla loro classe di protezione dati.

Portachiavi iCloud

Integrazione di Safari con il portachiavi iCloud
Per le password dei siti web, Safari può generare automaticamente stringhe casuali sicure dal punto di vista della codifica, che vengono archiviate nel portachiavi e sincronizzate sugli altri dispositivi. Gli elementi del portachiavi vengono trasferiti da un dispositivo all'altro attraverso i server Apple, ma sono codificati in modo che né Apple né altri dispositivi possano leggerne i contenuti.

Il portachiavi iCloud consente agli utenti di sincronizzare in maniera sicura le proprie password tra i dispositivi iOS e i computer Mac senza rivelare tali informazioni ad Apple. Oltre a un forte accento sulla privacy e la sicurezza, gli altri obiettivi che hanno influenzato sostanzialmente il design e l'architettura del portachiavi iCloud sono stati la semplicità d'uso e la possibilità di recuperare i portachiavi. Il portachiavi iCloud è composto da due servizi: la sincronizzazione e il recupero del portachiavi.

Apple ha progettato il portachiavi iCloud e il sistema di recupero in modo che le password dell'utente rimangano protette anche nei seguenti casi:

- Se l'account iCloud dell'utente viene compromesso.
- Se iCloud viene compromesso da un attacco esterno o da un dipendente.
- Una terza parte accede agli account utente.

Sincronizzazione del portachiavi

Quando l'utente crea per la prima volta un portachiavi iCloud, il dispositivo stabilisce una cerchia di attendibilità e crea una propria identità di sincronizzazione composta da una chiave pubblica e da una chiave privata. La chiave pubblica dell'identità di sincronizzazione viene inserita nella cerchia, che viene firmata due volte: prima dalla chiave privata dell'identità, poi con una chiave ellittica asimmetrica (con la curva P-256) derivata dalla password dell'account iCloud dell'utente. Nella cerchia vengono memorizzati anche i parametri (random salt e iterazioni) utilizzati per creare una chiave basata sulla password iCloud dell'utente.

La cerchia di sincronizzazione firmata è posizionata all'interno dell'area di archiviazione dei valori chiave di iCloud. Non è possibile leggerla senza conoscere la password iCloud dell'utente né modificarla in maniera valida senza la chiave privata dell'identità di sincronizzazione del suo membro.

Quando l'utente attiva il portachiavi iCloud su un altro dispositivo, questo rileva che l'utente è già presente in una cerchia di sincronizzazione di iCloud di cui il dispositivo non fa parte. Il dispositivo crea la propria coppia di chiavi per l'identità di sincronizzazione, quindi genera un ticket applicazione per richiedere di essere incluso nella cerchia. Il ticket consiste nella chiave pubblica dell'identità di sincronizzazione del dispositivo e all'utente viene chiesto di autenticarsi inserendo la password di iCloud. I parametri per la generazione della chiave ellittica vengono recuperati da iCloud e generano una chiave utilizzata per firmare il ticket applicazione. Per finire, il ticket applicazione viene inserito in iCloud.

Quando il primo dispositivo rileva l'arrivo di un ticket applicazione, visualizza un avviso per comunicare all'utente che un nuovo dispositivo ha richiesto di entrare nella cerchia di sincronizzazione. L'utente inserisce la password di iCloud, quindi il sistema verifica che il ticket applicazione sia firmato da una chiave privata corrispondente. In questo modo si stabilisce che la persona che ha generato la richiesta di aggiunta alla cerchia abbia contestualmente inserito la password iCloud dell'utente.

Quando l'utente approva l'inserimento del nuovo dispositivo nella cerchia, il primo dispositivo aggiunge la chiave pubblica del nuovo membro alla cerchia di sincronizzazione, quindi la firma nuovamente utilizzando sia la sua identità di sincronizzazione, sia la chiave derivata dalla password iCloud dell'utente. La nuova cerchia di sincronizzazione viene inserita in iCloud e firmata in maniera simile dal nuovo membro.

Ora nella cerchia di sincronizzazione ci sono due membri e ciascuno dispone della chiave pubblica dell'altro. A questo punto iniziano a scambiarsi singoli elementi del portachiavi attraverso l'archivio di valori chiave di iCloud o li archiviano in CloudKit a seconda dei casi. Se entrambi i membri hanno lo stesso elemento, viene sincronizzato quello con la data di modifica più recente. Se entrambi i membri hanno lo stesso elemento e la data di modifica coincide, l'elemento viene ignorato. Ogni elemento sincronizzato viene codificato in maniera tale che possa essere decodificato solo da un dispositivo che faccia parte della cerchia di attendibilità dell'utente. Non può essere decodificato da altri dispositivi né da Apple.

Questo processo si ripete per ogni nuovo dispositivo che entra nella cerchia. Ad esempio, quando viene aggiunto un terzo dispositivo, la conferma appare su entrambi gli altri dispositivi dell'utente, che potrà dare la propria approvazione da uno qualsiasi dei due dispositivi. Man mano che si aggiungono membri, ogni dispositivo si sincronizza con il nuovo arrivato per garantire che tutti dispongano degli stessi elementi del portachiavi.

Tuttavia non viene sincronizzato l'intero portachiavi: alcuni elementi, per esempio le identità VPN, sono specifici per il dispositivo e non devono quindi essere trasferiti. La sincronizzazione riguarda solo gli elementi con attributo `kSecAttrSynchronizable`. Apple ha impostato questo attributo per i dati utente di Safari (inclusi nomi utente, password e numeri di carte di credito) oltre che per le password Wi-Fi e le chiavi di codifica di HomeKit.

Inoltre, di default, non vengono sincronizzati gli elementi del portachiavi aggiunti da app di terze parti. Quando aggiungono elementi al portachiavi, gli sviluppatori devono impostare l'attributo `kSecAttrSynchronizable`.

Recupero del portachiavi

La funzionalità di recupero del portachiavi offre all'utente la possibilità di depositare il proprio portachiavi presso Apple, senza che Apple possa leggere le password e gli altri dati al suo interno. Anche per chi ha un solo dispositivo, la funzionalità di recupero del portachiavi funge da rete di sicurezza in caso di perdita dei dati. Si tratta di un aspetto particolarmente importante quando si utilizza Safari per generare password sicure casuali per gli account web, poiché tali password risiedono esclusivamente nel portachiavi.

Fattori fondamentali nel recupero del portachiavi sono l'autenticazione secondaria e un servizio di deposito sicuro, creato da Apple specificamente per questa funzionalità. Il portachiavi dell'utente viene codificato con una password sicura, inoltre il servizio di deposito ne fornirà una copia solo nel caso in cui sia rispettata una serie di condizioni molto precise.

Quando il portachiavi iCloud è attivo, se sull'account dell'utente è abilitata l'autenticazione a due fattori, verrà utilizzato il codice del dispositivo per recuperare un portachiavi depositato. Se l'autenticazione a due fattori non è configurata, all'utente viene richiesto di creare un codice di sicurezza di iCloud fornendo un codice di sei cifre. In alternativa, senza l'autenticazione

a due fattori, l'utente può specificare un codice più lungo oppure lasciare al dispositivo il compito di creare un codice crittograficamente casuale da annotare e conservare in un luogo sicuro.

A questo punto, il dispositivo esporta una copia del portachiavi dell'utente, lo codifica utilizzando le chiavi in una keybag asimmetrica e lo colloca nell'archivio dei valori chiave dell'utente su iCloud. La keybag viene cifrata con il codice di sicurezza iCloud dell'utente e la chiave pubblica del cluster HSM (modulo di sicurezza hardware) che archivierà il record di deposito. Questo diventerà il record di deposito iCloud dell'utente.

Se l'utente ha deciso di accettare un codice di sicurezza crittograficamente casuale anziché specificare il proprio codice o utilizzarne uno a quattro cifre, non è necessario alcun record di deposito: verrà utilizzato il codice di sicurezza di iCloud per cifrare direttamente la chiave casuale.

Oltre a stabilire un codice di sicurezza, gli utenti devono registrare un numero di telefono, che verrà utilizzato per un secondo livello di autenticazione durante il recupero del portachiavi. L'utente riceverà un SMS a cui dovrà rispondere prima di poter procedere.

Sicurezza del servizio di deposito

iCloud fornisce un'infrastruttura sicura per il deposito del portachiavi a garanzia che solo gli utenti e i dispositivi autorizzati possano effettuare un recupero. Dietro iCloud, vi sono i cluster HSM che proteggono i record depositati. Ciascuno dispone di una chiave utilizzata per codificare i record di propria competenza, come descritto in precedenza in questo documento.

Per recuperare un portachiavi, l'utente deve autenticarsi con l'account e la password di iCloud e rispondere al messaggio SMS inviato al numero di telefono registrato. Fatto questo, l'utente deve inserire il proprio codice di sicurezza iCloud. Il cluster HSM verifica che l'utente conosca il proprio codice di sicurezza iCloud utilizzando il protocollo Secure Remote Password (SRP); il codice non viene inviato ad Apple. Ogni membro del cluster verifica in modo indipendente che l'utente non abbia superato il numero massimo di tentativi consentiti per recuperare il proprio record, come spiegato in seguito. Se la maggioranza concorda, il cluster decifra il record depositato e lo invia al dispositivo dell'utente.

A questo punto il dispositivo utilizza il codice di sicurezza iCloud per decifrare la chiave casuale usata per codificare il portachiavi dell'utente. Con questa chiave, il portachiavi recuperato dall'archivio dei valori chiave di iCloud viene decodificato e ripristinato sul dispositivo. Sono consentiti 10 tentativi di autenticazione e recupero del record depositato. Dopo una serie di tentativi non riusciti, il record viene bloccato e l'utente deve contattare il Supporto Apple per poter effettuare ulteriori tentativi. Dopo il decimo tentativo non riuscito, il cluster HSM distrugge il record depositato e il portachiavi è perduto per sempre. Si tratta di una protezione contro gli attacchi di forza bruta volti a recuperare il record: in questo modo, i dati sono tutelati anche a costo di sacrificare il portachiavi.

Queste politiche sono codificate nel firmware HSM. Le schede di accesso amministrativo che permettono di modificare il firmware sono state distrutte. Qualsiasi tentativo di alterare il firmware o di accedere alla chiave privata causerà l'eliminazione della chiave privata da parte del cluster HSM. Se ciò dovesse verificarsi, il proprietario di ciascun portachiavi custodito dal cluster riceverà un messaggio che lo informa che il record depositato è andato perduto; potrà quindi scegliere di registrarsi nuovamente.

Siri

Semplicemente parlando in modo naturale, gli utenti possono chiedere a Siri di inviare messaggi, fissare appuntamenti, effettuare una telefonata e molto altro. Siri utilizza il riconoscimento vocale, la sintesi vocale e un modello client-server per rispondere a un'ampia gamma di richieste. Le operazioni supportate da Siri sono state progettate in modo da garantire che venga richiesto solo un quantitativo minimo di informazioni personali, che sono pienamente protette.

Quando attivi Siri, il dispositivo crea degli identificatori casuali da utilizzare con il riconoscimento vocale e con i server di Siri. Questi identificatori sono utilizzati solo all'interno di Siri per migliorare il servizio. Se in seguito si disattiva Siri, il dispositivo provvederà a generare un nuovo identificatore casuale da utilizzare nel caso in cui l'utente riattivi il servizio.

Per consentire l'uso delle funzionalità di Siri, alcune informazioni dell'utente vengono inviate al server, come ad esempio informazioni sulla libreria musicale (titoli dei brani, artisti e playlist), i nomi degli elenchi in Promemoria, nonché i nomi e le relazioni che l'utente ha definito in Contatti. Tutte le comunicazioni con il server avvengono via HTTPS.

Quando si avvia una sessione con Siri, il server riceve il nome e il cognome dell'utente (da Contatti), insieme alla posizione geografica approssimata per consentire a Siri di rivolgersi all'utente chiamandolo per nome o di rispondere a domande che richiedono di conoscere solo una posizione approssimata, come quelle relative al meteo.

Se è necessaria una posizione più precisa, per esempio per determinare l'ubicazione di un cinema nei paraggi, il server chiede al dispositivo di fornire coordinate più esatte. Questo è un esempio di come, di default, le informazioni vengano inviate al server solo quando è strettamente necessario per elaborare la richiesta dell'utente. In ogni caso, i dati della sessione sono eliminati dopo 10 minuti di inattività.

Quando una richiesta a Siri proviene da Apple Watch, l'orologio crea un proprio identificatore casuale univoco come descritto sopra. Tuttavia, anziché trasmettere di nuovo le informazioni dell'utente, la richiesta invia anche l'identificatore Siri dell'iPhone abbinato, che funge da riferimento.

La registrazione delle parole pronunciate dall'utente viene inviata al server di riconoscimento vocale di Apple. Se l'operazione si limita alla dettatura, il testo riconosciuto viene quindi restituito al dispositivo. Altrimenti, Siri analizza il testo e, se necessario, lo abbina alle informazioni contenute nel profilo associato al dispositivo. Per esempio, se l'utente chiede "Invia un messaggio alla mamma", il servizio utilizza le relazioni e i nomi che sono stati caricati da Contatti. Il comando per l'azione identificata viene quindi inviato al dispositivo per l'esecuzione.

Molte azioni di Siri sono completate dal dispositivo sotto la direzione del server. Ad esempio, se l'utente chiede a Siri di leggere un messaggio che ha ricevuto, il server comunica semplicemente al dispositivo di pronunciare i contenuti dei messaggi non letti. Contenuto e mittente del messaggio non vengono inviati al server.

Le registrazioni vocali sono conservate per sei mesi, in modo che il sistema di riconoscimento possa utilizzarle per capire meglio la voce dell'utente. Dopo sei mesi viene salvata un'altra copia, sprovvista di identificatore, che Apple potrà utilizzare per un massimo di due anni al fine di migliorare e sviluppare Siri. Un sottoinsieme ridotto di registrazioni, trascrizioni e dati associati senza identificatori potrebbe continuare a essere utilizzato

da Apple per il controllo di qualità e il miglioramento costanti di Siri per oltre due anni. Il sistema conserva anche alcune registrazioni che fanno riferimento a musica, squadre sportive e giocatori, attività commerciali o punti di interesse, sempre allo scopo di migliorare Siri.

È inoltre possibile accedere a Siri tramite attivazione vocale, senza usare le mani. Il rilevamento del comando vocale avviene localmente sul dispositivo. In questa modalità, Siri si attiva solo quando il modello vocale in ingresso corrisponde a sufficienza con l'acustica della frase di comando specificata. Al rilevamento del comando, l'audio corrispondente e il successivo comando Siri vengono inviati al server di riconoscimento vocale di Apple, che procede all'elaborazione seguendo le stesse regole delle registrazioni vocali effettuate dall'utente attraverso Siri.

Gli utenti possono anche attivare Siri su Apple Watch, sollevando l'orologio e avvicinandolo alla bocca per pronunciare una richiesta. Siri si attiva in questo modo quando si verificano queste due condizioni:

- Un modello di apprendimento automatico sul dispositivo rileva le caratteristiche acustiche del parlato umano vicino al dispositivo.
- Un secondo modello di apprendimento automatico sul dispositivo identifica un profilo di movimento e una posizione che corrispondono al gesto "Alza per parlare".

Al rilevamento di tale combinazione di movimento e audio, l'audio corrispondente viene inviato al server di riconoscimento vocale di Apple, che procede all'elaborazione seguendo le stesse regole delle registrazioni vocali effettuate dall'utente attraverso Siri.

Suggerimenti di Siri

I suggerimenti di Siri per le app e le abbreviazioni vengono generati tramite apprendimento automatico eseguito sul dispositivo. Nessun dato viene inviato a Apple, tranne le informazioni che non possono essere utilizzate per identificare l'utente riguardo a quali segnali sono stati utili a predire abbreviazioni o avvii di app.

Abbreviazioni in Siri

Le abbreviazioni aggiunte a Siri vengono sincronizzate su tutti i dispositivi Apple tramite iCloud e sono codificate tramite la codifica end-to-end di CloudKit. Le frasi associate alle abbreviazioni vengono archiviate sul server di Siri per il riconoscimento vocale e associate all'identificatore casuale di Siri descritto nella sezione Siri. Apple non riceve i contenuti delle abbreviazioni, che sono archiviati localmente in un contenitore sicuro di dati.

App Comandi Rapidi

I comandi personalizzati dell'app Comandi Rapidi sono facoltativamente sincronizzati tra i dispositivi Apple tramite iCloud. I comandi possono anche essere condivisi con altri utenti tramite iCloud.

I comandi personalizzati sono versatili, sono simili a script o programmi. Per isolare i comandi scaricati da Internet viene utilizzato un sistema di quarantena. L'utente viene avvisato la prima volta che cerca di usare il comando e gli viene data la possibilità di esaminarlo, controllando anche le informazioni sulla sua origine.

I comandi personalizzati possono eseguire anche JavaScript specificati dall'utente sui siti web in Safari, quando avviati dalla finestra di condivisione. Per proteggere da JavaScript dannosi che, ad esempio, potrebbero indurre l'utente ad eseguire uno script sul sito di un social

media per raccogliere i suoi dati, durante l'esecuzione vengono scaricate definizioni aggiornate sui malware per identificare gli script dannosi. La prima volta che esegue un JavaScript su un dominio, all'utente viene richiesto di consentire ai comandi contenenti JavaScript di venire eseguiti sulla pagina web attuale del dominio.

Suggerimenti di Safari, suggerimenti di Siri nella ricerca, Cerca, #immagini, l'app News e il widget News nei paesi in cui News non è supportato

I suggerimenti di Safari, i suggerimenti di Siri nella ricerca, Cerca, #immagini, l'app News e il widget News nei paesi in cui News non è supportato mostrano agli utenti dei suggerimenti che attingono a fonti al di fuori dei loro dispositivi, come Wikipedia, iTunes Store, i siti locali di notizie, i risultati di Mappe e App Store; inoltre, forniscono dei suggerimenti persino prima che l'utente inizi a digitare.

Quando un utente inizia a digitare nella barra degli indirizzi di Safari, apre o utilizza i suggerimenti di Siri, usa Cerca, apre #immagini, utilizza la ricerca nell'app News o usa il widget News nei paesi in cui News non è supportato, le informazioni di contesto seguenti vengono inviate ad Apple in forma codificata tramite HTTPS per fornire all'utente dei risultati pertinenti:

- Un identificatore che cambia ogni 15 minuti per tutelare la privacy.
- Query di ricerca dell'utente.
- Il completamento più probabile della domanda di ricerca in base al contesto e alle ricerche precedenti salvate nella cache locale.
- La posizione approssimativa del dispositivo, se sono abilitati i servizi di localizzazione per i suggerimenti basati sulla posizione. Il livello di "offuscamento" della posizione si basa sulla densità di popolazione nella posizione del dispositivo; per esempio, l'offuscamento è maggiore nelle località rurali, in cui gli utenti potrebbero essere maggiormente distanziati geograficamente, rispetto ai centri metropolitani, dove gli utenti sono tipicamente più vicini. Gli utenti possono disabilitare l'invio ad Apple delle informazioni sulla posizione in Impostazioni, disattivando i servizi di localizzazione per i suggerimenti basati sulla posizione. Se i servizi di localizzazione sono disattivati, Apple potrebbe utilizzare l'indirizzo IP del dispositivo per rilevarne la posizione approssimativa.
- Il tipo di dispositivo e se la ricerca viene effettuata tramite i suggerimenti di Siri, nella ricerca, in Safari, in Cerca, nell'app News o in Messaggi.
- Il tipo di connessione.
- Le informazioni sulle tre app utilizzate più di recente sul dispositivo (usate per fornire ulteriore contesto per la ricerca). Vengono incluse solo le app che rientrano in un elenco di titoli popolari stilato da Apple e che sono state utilizzate nelle ultime tre ore.
- Un elenco delle app popolari presenti sul dispositivo.
- Lingua regionale, impostazioni locali e preferenze di input.
- Se il dispositivo dell'utente ha accesso a servizi di abbonamento a musica e video, informazioni come il nome del servizio e il tipo di abbonamento potrebbero essere inviati ad Apple. Il nome dell'account, il numero e la password dell'utente non sono inviati ad Apple.
- Una rappresentazione ridotta e sintetizzata degli argomenti di interesse.

Quando un utente seleziona un risultato o esce dall'app senza selezionarne nessuno, vengono inviate ad Apple alcune informazioni tese al miglioramento della qualità dei risultati futuri. Tali informazioni sono vincolate solo allo stesso identificatore della sessione di 15 minuti e non a un utente in particolare. Il feedback include alcune delle informazioni di contesto descritte sopra e informazioni relative alle interazioni come ad esempio:

- Misurazione del tempo intercorso fra le interazioni e le richieste di ricerca sulla rete.
- Classificazione e ordine di visualizzazione dei suggerimenti.
- L'ID del risultato e dell'azione selezionata se il risultato non è locale oppure, in caso di risultato locale, la categoria a cui appartiene.
- Un contrassegno che indica se l'utente ha selezionato il risultato.

Apple conserva i log dei suggerimenti insieme a richieste, contesto e feedback per 18 mesi. Un sottoinsieme di log viene conservato per un periodo massimo di 5 anni e comprende, ad esempio, le domande di ricerca, le impostazioni regionali, il dominio, la posizione approssimativa e un insieme di misurazioni.

In alcuni casi, i suggerimenti possono inoltrare le richieste relative a parole e frasi comuni a partner qualificati, al fine di ricevere e visualizzare i risultati di ricerca del partner. Apple gestisce le domande tramite proxy, in modo che i partner non ricevano l'indirizzo IP dell'utente o il feedback della ricerca. La comunicazione con i partner viene codificata tramite HTTPS. Per le richieste frequenti, Apple fornisce la posizione geografica dell'utente, il tipo di dispositivo e la lingua del cliente come informazioni sul contesto della ricerca per migliorare le prestazioni di ricerca.

Per comprendere e migliorare le prestazioni di ricerca dal punto di vista geografico e tra diversi tipi di rete, vengono incluse nei log le seguenti informazioni (senza identificatore di sessione):

- Indirizzo IP parziale (senza gli ultimi 8 caratteri nel caso degli indirizzi IPv4 e senza gli ultimi 80 bit nel caso degli indirizzi IPv6)
- Posizione approssimata.
- Ora approssimata della richiesta.
- Latenza/velocità di trasferimento.
- Dimensioni della risposta.
- Tipo di connessione.
- Impostazioni regionali.
- Tipo di dispositivo e app che realizza la richiesta.

Prevenzione intelligente del tracciamento di Safari

La prevenzione intelligente del tracciamento, o ITP (Intelligent Tracking Prevention) fa parte della politica di default di Safari relativa a cookie e dati dei siti web che mira a salvaguardare la privacy. Aiuta a impedire il tracciamento tra siti limitando l'accesso ai cookie e ad altri dati dei siti web.

ITP raccoglie le statistiche sul caricamento delle risorse (immagini, script etc) e sulle interazioni dell'utente come tocchi e inserimento di testo. Viene utilizzato un modello di apprendimento automatico sul dispositivo che classifica quali nomi dominio possono tracciare l'utente tra un sito e l'altro, in base alle statistiche raccolte.

Quando un dominio viene classificato come in grado di tracciare l'utente, ITP suddivide immediatamente i cookie se l'utente ha precedentemente interagito con il dominio come prima parte; per i domini classificati con cui l'utente non ha interagito, ITP inizia immediatamente a bloccare i cookie. Ad esempio:

- video.example offre un servizio in abbonamento senza pubblicità e ha molti dei propri video integrati in altri siti web.
- Un utente accede a video.example e successivamente ad altri siti web che presentano i contenuti integrati di video.example.
- ITP classifica video.example come in grado di tracciare l'utente, quindi ne suddivide i cookie.
- Quando un utente visita quotidiano.example e questo presenta contenuti integrati da video.example, i cookie forniti a video.example sono cookie suddivisi specifici per video.example su newspaper.example.

I contenuti integrati di terze parti potrebbero richiedere all'utente l'accesso ai suoi cookie di prima parte con l'API Storage Access. Quando un utente tocca o fa clic su un contenuto integrato di terze parti che usa l'API Storage Access, Safari mostra un avviso che chiede se l'utente vuole consentire alla terza parte di accedere ai suoi cookie e dati dei siti web, il che consente alla terza parte di tracciarlo sul dominio di prima parte. Se l'utente seleziona Consenti, al contenuto integrato di terze parti è permesso di accedere ai cookie della prima parte per la durata della visita alla pagina; nelle visite successive, il contenuto integrato di terze parti avrà accesso ai cookie della prima parte dopo che l'utente avrà interagito con il contenuto integrato e questo avrà richiamato l'API Storage Access. E dal momento che l'utente ha precedentemente consentito questo accesso, non verrà mostrato alcun avviso. La decisione dell'utente riguardo alla combinazione tra prima parte e terze parti viene mantenuta e viene eliminata solo quando viene cancellata la cronologia di Safari.

I cookie esistenti dai domini classificati come in grado di tracciare l'utente vengono eliminati se l'utente non interagisce con il dominio (direttamente o tramite l'API Storage Access) per 30 giorni di uso attivo di Safari. Dopo 30 giorni senza interazione, un dominio classificato come in grado di tracciare l'utente non potrà neppure impostare nuovi cookie. Safari non consente mai l'accesso ai dati di siti web di prime parti in contesti di terze parti.

Attraverso l'isolamento di ITP dei dati di prime parti e di terze parti, è possibile una maggiore prevenzione dell'utilizzo dei cookie e dei dati dei siti web per il tracciamento tra un sito e l'altro. Apple non ha accesso a quali nomi dominio hanno fornito statistiche al dispositivo o sono stati classificati come in grado di tracciare l'utente.

Oltre a bloccare i cookie di terze parti da domini classificati come in grado di tracciare l'utente, ITP riduce le informazioni sul referer HTTP inviate ai domini classificati come in grado di tracciare l'utente, limitandole alla sola origine della pagina.

Gestione delle password dell'utente

iOS offre una varietà di funzionalità che facilitano l'autenticazione sicura ad app di terze parti e siti web che utilizzano le password per l'accesso. Le password vengono salvate in uno speciale portachiavi per il riempimento automatico, controllato dall'utente e gestibile da Impostazioni > Password e account >Password app e siti web. Le app non possono accedere al portachiavi per il riempimento automatico senza il permesso dell'utente. Le credenziali salvate su tale portachiavi vengono sincronizzate tra i dispositivi tramite il portachiavi iCloud, se abilitato.

Il portachiavi iCloud e il riempimento automatico delle password forniscono le seguenti funzionalità:

- Riempimento credenziali in app e siti web.
- Generazione di password sicure.
- Salvataggio di password in app e siti web su Safari.
- Condivisione sicura delle password verso i contatti dell'utente.
- Invio di password a un'Apple TV vicina che richiede delle credenziali.

Accesso delle app alle password salvate

API per le credenziali web condivise

Le app di iOS possono interagire con il portachiavi per il riempimento automatico delle password tramite le seguenti API:

`SecRequestSharedWebCredential`

`SecAddSharedWebCredential`

L'accesso è concesso alle app iOS solo se lo sviluppatore dell'app e l'amministratore del sito web hanno dato la loro approvazione e se l'utente ha espresso il proprio consenso. Gli sviluppatori di app esprimono la loro intenzione di accedere alle password salvate in Safari includendo un'approvazione nell'app. L'approvazione elenca i nomi dominio completi dei siti web associati e i siti web devono posizionare un file sul proprio server che elenchi gli identificatori unici delle app approvate da Apple.

Quando viene installata un'app con autorizzazione per i domini associati a com.apple.developer, iOS rivolge a ogni sito web elencato una richiesta TLS, chiedendo uno dei seguenti file:

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

Se l'elenco contenuto nel file comprende l'identificatore dell'app che viene installata, iOS segna la relazione tra il sito web e l'app come affidabile. Solo le relazioni di fiducia con chiamate a queste due API risulteranno in una richiesta rivolta all'utente che dovrà esprimere il proprio consenso prima che qualsiasi password venga rilasciata all'app, venga aggiornata o eliminata.

Riempimento automatico delle password per le app

iOS consente agli utenti di inserire i nomi utente e le password nei campi per la richiesta delle credenziali nelle app toccando un apposito tasto nella barra QuickType della tastiera di iOS. Viene sfruttato lo stesso meccanismo di associazione forte che utilizza il file apple-app-site-association per legare app e siti web. Questa interfaccia non rivela nessuna informazione sulle credenziali all'app finché un utente non ne consente il rilascio. Se iOS contrassegna come attendibile la relazione fra un sito web e un'app, la barra QuickType mostra direttamente anche le credenziali da inserire nell'app. Questo consente agli utenti di rivelare alle app le credenziali salvate tramite Safari, con le stesse proprietà di sicurezza, ma senza che le app debbano adottare un'API.

Quando un'app e un sito web hanno una relazione attendibile e un utente invia le credenziali in un'app, iOS potrebbe chiedere all'utente di salvarle nel portachiavi per il riempimento automatico delle password per un uso successivo.

Password sicure automatiche

Quando il portachiavi iCloud è abilitato, iOS crea password uniche, casuali, sicure quando gli utenti accedono o modificano la password in un'app o in un sito web in Safari. Per non utilizzare le password sicure, gli utenti devono disattivare l'opzione. Le password generate vengono salvate nel portachiavi e sincronizzate tra i dispositivi tramite il portachiavi iCloud, se abilitato.

Le password generate da iOS, di default, contengono 20 caratteri. Esse contengono una cifra, un carattere maiuscolo, due trattini e 16 caratteri minuscoli. Si tratta di password sicure, contenenti 71 bit di entropia.

iOS genera le password nelle app e in Safari in base a dati euristici che determinano se il contesto è adatto alla creazione di una password. Se la determinazione euristica non riesce a identificare il contesto adatto alla creazione di una password, gli sviluppatori delle app possono impostare UITextContentType.newPassword sul campo di testo e gli sviluppatori web possono impostare autocomplete="new-password" sugli elementi <input>.

Le app e i siti web possono fornire delle regole a iOS per garantire che le password generate siano compatibili con un determinato servizio. iOS genererà la password più forte che possa soddisfare tali regole. Gli sviluppatori forniscono tali regole tramite l'attributo UITextInputPasswordRules o passwordrules sugli elementi <input>.

Invio delle password ad altre persone o dispositivi

AirDrop

Quando iCloud è abilitato, gli utenti possono inviare tramite AirDrop le credenziali salvate, inclusi i siti web per cui sono salvate, il nome utente e la password a un altro dispositivo. L'invio delle credenziali con AirDrop funziona sempre in modalità "Solo contatti", a prescindere dalle impostazioni dell'utente. (Consulta "Sicurezza di AirDrop" per ulteriori informazioni). Sul dispositivo ricevente, dopo il consenso dell'utente, le credenziali verranno archiviate nel portachiavi per il riempimento automatico delle password.

Apple TV

Il riempimento automatico delle password è disponibile per inserire le credenziali nelle app su Apple TV. Quando l'utente seleziona un campo di testo per nome utente o password in tvOS, Apple TV inizia a trasmettere una richiesta per il riempimento automatico della password tramite BLE (Bluetooth Low Energy).

Qualsiasi iPhone nelle vicinanze mostrerà una richiesta che invita l'utente a condividere le credenziali con Apple TV. Durante questa procedura, un iPhone e un'Apple TV che usano lo stesso account di iCloud codificano la comunicazione tra i due dispositivi. Se iPhone è connesso a un account di iCloud di verso da quello di Apple TV:

- Per stabilire una connessione codificata viene utilizzato un codice PIN.
- iPhone deve essere sbloccato e vicino al telecomando Siri Remote abbinato a Apple TV per ricevere la richiesta.

Una volta effettuata la connessione codificata tramite Bluetooth Low Energy, le credenziali vengono inviate a Apple TV e vengono automaticamente inserite nei campi di testo appropriati sull'app.

Estensioni per la fornitura di credenziali

Gli utenti possono designare un'applicazione di terze parti compatibile come fornitore di credenziali per il riempimento automatico nelle impostazioni "Password e account". Questo meccanismo si basa sulle estensioni. L'estensione fornitrice di credenziali deve prevedere una schermata per scegliere le credenziali e può facoltativamente fornire a iOS dei metadati sulle credenziali salvate, in modo che possano essere offerte direttamente nella barra QuickType. I metadati includono il sito web delle credenziali e il nome utente associato, ma non la password. iOS comunicherà con l'estensione per ottenere la password quando l'utente sceglie di inserirla in un'app o in un sito su Safari. I metadati delle credenziali sono archiviati nella sandbox del fornitore di credenziali e vengono rimossi automaticamente quando un'app viene disinstallata.

Controlli del dispositivo

iOS supporta configurazioni e politiche di sicurezza flessibili, facili da applicare e da gestire. Ciò permette alle organizzazioni di proteggere le informazioni aziendali e di assicurarsi che i dipendenti rispettino i requisiti dell'azienda anche quando utilizzano dispositivi di loro proprietà, come nel caso di un programma BYOD (Bring Your Own Device).

Le organizzazioni possono utilizzare risorse come la protezione con codice, i profili di configurazione, la cancellazione a distanza e le soluzioni MDM di terze parti per gestire le flotte di dispositivi e favorire la protezione dei dati aziendali, anche quando i dipendenti vi accedono dai propri dispositivi iOS personali.

Protezione con codice

Di default, il codice si può definire come un PIN numerico. Sui dispositivi con Touch ID o Face ID, la lunghezza minima del codice è di quattro cifre. Gli utenti possono specificare un codice alfanumerico più lungo selezionando "Codice alfanumerico personalizzato" nelle opzioni relative al codice in Impostazioni > Codice. I codici più lunghi e complessi sono più difficili da indovinare o da attaccare e sono consigliati.

Gli amministratori possono imporre l'uso di codici complessi e altre politiche utilizzando soluzioni MDM o Exchange ActiveSync, oppure chiedendo agli utenti di installare manualmente dei profili di configurazione. Sono disponibili le seguenti politiche per il codice:

- Consenti valore semplice.
- Richiedi valore alfanumerico.
- Lunghezza minima del codice.
- Numero minimo di caratteri complessi.
- Tempo massimo di validità del codice.
- Cronologia dei codici.
- Intervallo di tempo prima del blocco automatico.
- Intervallo per il blocco del dispositivo.
- Numero massimo di tentativi non riusciti.
- Consenti Touch ID o Face ID.

Per i dettagli utili agli amministratori per ciascuna politica, consulta: https://help.apple.com/deployment/mdm/#/mdm4D6A472A

Per i dettagli utili agli sviluppatori per ciascuna politica, consulta: https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/

Modello di abbinamento di iOS

iOS utilizza un modello di abbinamento per controllare l'accesso al dispositivo da un computer host. L'abbinamento instaura una relazione attendibile fra il dispositivo e l'host connesso, indicata da uno scambio di chiavi pubbliche. iOS utilizza questa firma di attendibilità per abilitare ulteriori funzionalità con l'host connesso, come la sincronizzazione dei dati.

In iOS 9, i servizi che richiedono un abbinamento non possono essere avviati finché il dispositivo non viene sbloccato dall'utente.

Inoltre, in iOS 10 o versioni successive, alcuni servizi, compresa la sincronizzazione delle foto, richiedono che il dispositivo sia sbloccato per potere iniziare.

In iOS 11 o versioni successive, i servizi non si avviano a meno che il dispositivo non sia stato sbloccato di recente.

In fase di abbinamento l'utente deve sbloccare il dispositivo e accettare la richiesta proveniente dall'host. In iOS 11 o versioni successive, all'utente viene anche chiesto di inserire il codice. Completato questo passaggio, l'host e il dispositivo si scambiano e salvano le chiavi pubbliche RSA a 2048 bit. L'host riceve quindi una chiave a 256 bit che può sbloccare la keybag Escrow archiviata sul dispositivo (consulta “Keybag Escrow” nella sezione Keybag di questo documento). Le chiavi scambiate vengono utilizzate per iniziare una sessione SSL codificata, richiesta dal dispositivo prima di inviare dati protetti all'host o prima di avviare un servizio (sincronizzazione iTunes, trasferimento di file, sviluppo Xcode ecc.). Il dispositivo richiede che le connessioni Wi-Fi da un host utilizzino questa sessione codificata per tutte le comunicazioni, pertanto deve essere stato abbinato in precedenza via USB. L'abbinamento abilita anche una serie di funzionalità di diagnostica. In iOS 9, se un record di abbinamento non è stato utilizzato per più di sei mesi, viene considerato scaduto. Questo periodo di tempo è ridotto a 30 giorni in iOS 11 o versioni successive.

Per ulteriori informazioni, consulta: https://support.apple.com/HT6331

Alcuni servizi, tra cui com.apple.pcapd, possono solo funzionare via USB. Inoltre, il servizio com.apple.file_relay richiede che sia installato un profilo di configurazione firmato da Apple.

In iOS 11 o versioni successive, Apple TV può utilizzare il protocollo Secure Remote Password per stabilire una relazione di abbinamento in modalità wireless.

L'utente può azzerare l'elenco degli host attendibili utilizzando le opzioni “Ripristina impostazioni rete” o “Ripristina posizione e privacy”.

Per ulteriori informazioni, consulta: https://support.apple.com/HT5868

Imposizione delle configurazioni

Un profilo di configurazione è un file XML che consente a un amministratore di distribuire informazioni di configurazione ai dispositivi iOS. Le impostazioni definite da un profilo di configurazione installato non possono essere modificate dall'utente. Se l'utente elimina un profilo di configurazione, vengono rimosse anche tutte le impostazioni definite dal profilo. In questo modo gli amministratori possono applicare impostazioni definendo politiche per il Wi-Fi e l'accesso ai dati. Ad esempio, un profilo di configurazione che fornisce una configurazione e-mail può anche specificare una politica per il codice del dispositivo. Gli utenti saranno in grado di accedere alle e-mail solo se il codice soddisfa i requisiti dell'amministratore.

Un profilo di configurazione iOS permette di specificare una varietà di impostazioni, tra cui:

- Politiche per il codice.
- Restrizioni per le funzionalità del dispositivo (per esempio, disabilitare la fotocamera).
- Impostazioni Wi-Fi.
- Impostazioni VPN.
- Impostazioni dei server di posta.
- Impostazioni di Exchange.
- Impostazioni del servizio di directory LDAP.
- Impostazioni del servizio di calendario CalDAV.
- Clip web.
- Credenziali e chiavi.
- Impostazioni avanzate della rete cellulare.

Per visualizzare un elenco attuale per gli amministratori, consulta: https://help.apple.com/deployment/mdm/#/mdm5370d089

Per visualizzare un elenco attuale per gli sviluppatori, consulta: https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/

È possibile firmare e codificare i profili di configurazione per confermarne l'origine, assicurarne l'integrità e proteggerne il contenuto. I profili di configurazione sono codificati tramite CMS (RFC 3852), con supporto per 3DES e AES-128.

Inoltre è possibile bloccare i profili di configurazione su un dispositivo per impedirne la rimozione, o per consentirla solo inserendo un codice. Dato che molti utenti aziendali sono i proprietari dei dispositivi iOS che utilizzano, è possibile rimuovere i profili di configurazione che legano un dispositivo a una soluzione MDM. Tuttavia questo fa in modo che vengano rimosse anche tutte le informazioni, le app e i dati gestiti.

Gli utenti possono installare i profili di configurazione direttamente sui dispositivi tramite Apple Configurator 2; in alternativa, i profili possono essere scaricati tramite Safari, inviati per e-mail o in modalità wireless tramite una soluzione MDM. Quando un utente configura un dispositivo in Apple School Manager o Apple Business Manager, il dispositivo scarica e installa un profilo per la registrazione MDM.

Gestione dei dispositivi mobili (MDM)

Il supporto MDM di iOS consente alle aziende di configurare e gestire in maniera sicura distribuzioni scalate di iPhone, iPad, Apple TV e Mac all'interno delle proprie organizzazioni. Le funzionalità MDM sono integrate nelle tecnologie iOS esistenti come i profili di configurazione, la registrazione in modalità wireless e il servizio Apple Push Notification (APN). Ad esempio, il servizio di notifiche push di Apple è utilizzato per attivare il dispositivo e consentire così la comunicazione diretta con la soluzione MDM tramite una connessione protetta. Nessuna informazione confidenziale o proprietaria viene trasmessa via APN.

Utilizzando MDM, i reparti IT possono registrare i dispositivi iOS in un ambiente aziendale, configurare e aggiornare le impostazioni in modalità wireless, monitorare la conformità con le politiche aziendali, gestire le politiche di aggiornamento del software e perfino cancellare o bloccare a distanza i dispositivi gestiti.

Per ulteriori informazioni sull'uso delle soluzioni MDM, consulta:

- https://www.apple.com/it/iphone/business/it/management.html
- https://help.apple.com/deployment/ios/#/ior07301dd60
- https://help.apple.com/deployment/mdm/#/mdmbf9e668

iPad condiviso

"iPad condiviso" è una modalità multiutente per l'uso di iPad in contesti educativi. Consente agli studenti di condividere lo stesso iPad senza condividere però documenti e dati. A ogni studente viene fornita una directory Inizio, creata come volume APFS protetto dalle credenziali dell'utente. Per usare "iPad condiviso" occorre disporre di un ID Apple gestito emesso dall'ente educativo e di proprietà di tale ente. La modalità "iPad condiviso" consente allo studente di accedere a qualsiasi dispositivo, di proprietà del centro, che sia stato configurato per essere usato da più studenti. I dati dello studente vengono suddivisi in cartelle Inizio separate, ognuna delle quali si trova nel proprio dominio di protezione dati ed è protetta da permessi UNIX e sandbox.

Accedere a "iPad condiviso"

Quando uno studente effettua l'accesso, l'ID Apple gestito viene autenticato sui server di identità di Apple tramite il protocollo SRP. Se l'autenticazione avviene correttamente, al dispositivo viene assegnato un token specifico di breve durata per l'accesso. Se uno studente ha già utilizzato il dispositivo, dispone già di un account utente locale, che viene sbloccato tramite le stesse credenziali.

Se invece non ha mai utilizzato il dispositivo prima, riceve un nuovo ID utente UNIX, un volume APFS contenente la directory Inizio dell'utente e un portachiavi logico. Se il dispositivo non è connesso a Internet (ad esempio perché lo studente si trova in un'uscita didattica), l'autenticazione può verificarsi sull'account locale per un numero limitato di giorni. In una situazione di questo tipo possono accedere solo gli utenti che dispongono di account locali preesistenti. Una volta scaduto il tempo limite, agli studenti viene richiesto di effettuare l'autenticazione in linea, anche se esiste già un account locale.

Una volta creato o sbloccato l'account locale dello studente, se l'autenticazione è avvenuta da remoto, il token di breve durata emesso dai server di Apple viene trasformato in un token di iCloud che consente l'accesso a iCloud. A continuazione, vengono ripristinate le impostazioni dello studente e i suoi dati e documenti vengono sincronizzati da iCloud.

Mentre è attiva la sessione dello studente e il dispositivo è in linea, i documenti e i dati vengono archiviati su iCloud nel momento stesso in cui vengono creati o modificati. Inoltre, un meccanismo di sincronizzazione attivo in background garantisce che quando lo studente ha effettuato il logout le modifiche vengano inviate a iCloud. Una volta completata la sincronizzazione in background per l'utente, il relativo volume APFS viene disattivato e non potrà essere riattivato se non con le credenziali dell'utente.

Uscire da "iPad condiviso"

Quando uno studente esce da "iPad condiviso", la sua keybag utente viene immediatamente bloccata e tutte le app vengono chiuse. Per accelerare l'accesso di un nuovo studente, il sistema rinvia momentaneamente alcune azioni ordinarie di logout e presenta allo studente una nuova finestra di login. Se uno studente accede durante questo intervallo di tempo (circa 30 secondi) "iPad condiviso" esegue le operazioni rinviate come parte della procedura di accesso all'account del nuovo studente. Tuttavia, se "iPad condiviso" rimane inattivo, le azioni di chiusura rinviate vengono eseguite. Durante la fase di chiusura, la finestra di login viene riavviata come se si fosse verificato un altro logout.

Aggiornamenti di "iPad condiviso"

Quando un iPad condiviso viene aggiornato alla versione 10.3 o successiva da una versione precedente, viene effettuata una conversione una tantum del file system per rendere la partizione dati HFS+ un volume APFS. Se in qualsiasi momento sul sistema sono presenti delle directory Inizio, rimarranno sul volume dati principale invece di essere convertite in volumi APFS individuali.

Quando altri studenti effettueranno l'accesso, anche le relative directory Inizio verranno posizionate sul volume dati principale. I nuovi account utente non verranno creati con il loro volume APFS, come descritto precedentemente, finché non verranno eliminati tutti gli account utente sul volume dati principale. Dunque, per garantire a tutti gli utenti le protezioni e quote aggiuntive offerte da APFS, occorrerà aggiornare iPad alla versione 10.3 o successive tramite un'inizializzazione e reinstallazione oppure occorrerà eliminare tutti gli account utente dal dispositivo utilizzando l'apposito comando tramite una soluzione MDM.

Per ulteriori informazioni su "iPad condiviso", consulta:
https://help.apple.com/deployment/mdm/#/cad7e2e0cf56

Apple School Manager

Apple School Manager è un servizio per gli enti educativi che consente di acquistare contenuti, configurare la registrazione automatica dei dispositivi in soluzioni MDM, creare account per studenti e personale nonché di configurare corsi di iTunes U. Apple School Manager è accessibile dal web ed è progettato per manager e amministratori IT, personale e docenti.

Per ulteriori informazioni su Apple School Manager, consulta: https://help.apple.com/schoolmanager/

Apple Business Manager

Apple Business Manager è un portale web di facile utilizzo che consente agli amministratori IT di distribuire dispositivi iOS, macOS e tvOS da un unico ambiente. Quando utilizzato con una soluzione MDM, è possibile configurare le impostazioni dei dispositivi e acquistare e distribuire app e libri. Apple Business Manager è accessibile dal web ed è progettato per gli amministratori IT.

Per ulteriori informazioni su Apple Business Manager, consulta: https://help.apple.com/businessmanager/

Registrazione dispositivi

Apple School Manager e Apple Business Manager permettono di distribuire in maniera efficiente i dispositivi iOS che un'organizzazione ha acquistato direttamente da Apple o tramite rivenditori e gestori autorizzati Apple. I dispositivi con iOS 11 o versione successiva e tvOS 10.2 o versione successiva possono essere aggiunti a Apple School Manager e Apple Business Manager anche dopo l'acquisto, utilizzando Apple Configurator 2.

Le organizzazioni possono registrare automaticamente i dispositivi a una soluzione MDM senza doverli toccare o preparare materialmente prima di consegnarli agli utenti. Una volta registrati in uno dei programmi, gli amministratori accedono al relativo sito web e collegano il programma alla propria soluzione MDM. I dispositivi che hanno acquistato possono quindi essere assegnati agli utenti via MDM. Durante la procedura di configurazione del dispositivo, le sicurezza dei dati sensibili può essere aumentata applicando apposite misure di sicurezza. Ad esempio:

- Fare in modo che gli utenti effettuino l'autenticazione durante il flusso di configurazione iniziale in Impostazione Assistita sul dispositivo Apple durante l'attivazione.
- Fornire una configurazione preliminare con accesso limitato e richiedere una configurazione aggiuntiva del dispositivo per accedere ai dati sensibili.

Una volta assegnato un utente, il sistema installa automaticamente ogni eventuale configurazione, restrizione o controllo che è stato specificato tramite la soluzione MDM. Tutta la comunicazione tra i dispositivi e i server Apple è codificata tramite HTTPS (SSL).

È possibile semplificare ulteriormente il processo di configurazione eliminando passaggi specifici in Impostazione Assistita per iOS, tvOS e macOS, in modo che l'utente possa essere operativo in poco tempo. Gli amministratori possono anche controllare se l'utente può o non può rimuovere il profilo MDM dal dispositivo e assicurarsi che le restrizioni siano applicate al dispositivo fin dall'inizio. Una volta rimosso dalla confezione

e attivato, il dispositivo potrà essere registrato nel sistema MDM dell'organizzazione e l'utente troverà impostazioni di gestione, app e libri già installati.

Apple Configurator 2

In aggiunta alle soluzioni MDM, Apple Configurator 2 per macOS semplifica la configurazione e la preimpostazione di dispositivi iOS e Apple TV prima della consegna agli utenti. Con Apple Configurator 2, i dispositivi possono essere preconfigurati rapidamente con app, dati, restrizioni e impostazioni.

Apple Configurator 2 consente di utilizzare Apple School Manager o Apple Business Manager per registrare i dispositivi ad una soluzione (MDM) senza che gli utenti debbano ricorrere a Impostazione Assistita. Apple Configurator 2 può essere utilizzato anche per aggiungere dispositivi iOS e Apple TV a Apple School Manager o Apple Business Manager in seguito all'acquisto.

Per ulteriori informazioni su Apple Configurator 2, consulta: https://help.apple.com/configurator/mac/

Supervisione

Durante la configurazione di un dispositivo, un'organizzazione può decidere di supervisionarlo. La supervisione denota che il dispositivo è di proprietà dell'organizzazione e in questo modo è possibile ottenere un controllo aggiuntivo sulla configurazione e sulle restrizioni. Con Apple School Manager o Apple Business Manager la supervisione può essere abilitata in modalità wireless sul dispositivo, come parte della registrazione MDM o abilitata manualmente tramite Apple Configurator 2. Per supervisionare un dispositivo è necessario inizializzarlo e reinstallare il sistema operativo.

Per maggiori informazioni sulla configurazione e la gestione dei dispositivi iOS e Apple TV tramite una soluzione MDM o Apple Configurator 2, consulta: https://help.apple.com/deployment/ios/

Restrizioni

Le restrizioni possono essere abilitate, e in alcuni casi disabilitate, dagli amministratori per impedire agli utenti di accedere ad app, servizi o funzionalità specifiche del dispositivo. Le restrizioni vengono inviate ai dispositivi in un apposito payload, allegato a un profilo di configurazione e possono essere applicate ai dispositivi iOS, tvOS e macOS. Alcune restrizioni su un iPhone gestito potrebbero essere applicate anche a un Apple Watch abbinato.

Per visualizzare un elenco attuale per i gestori IT, consulta: https://help.apple.com/deployment/mdm/#/mdm0F7DD3D8

Inizializzazione remota

L'amministratore o l'utente può cancellare a distanza i contenuti dei dispositivi iOS. L'inizializzazione remota istantanea è ottenuta eliminando in modo sicuro la chiave di codifica per il blocco della memoria dalla Effaceable Storage, rendendo illeggibili tutti i dati. Il comando di inizializzazione a distanza può essere inviato tramite MDM, Exchange o iCloud.

Quando il comando è attivato dal server MDM o da iCloud, il dispositivo invia una conferma e procede all'inizializzazione. Per l'inizializzazione a distanza con Exchange, il dispositivo accede al server Exchange prima di avviare l'inizializzazione.

Gli utenti possono anche cancellare i dispositivi in loro possesso utilizzando l'app Impostazioni. Come accennato in precedenza, è possibile impostare i dispositivi in modo da avviare automaticamente la cancellazione dopo una serie di tentativi non riusciti di inserimento del codice.

Modalità smarrito

Se un dispositivo viene perso o rubato, un amministratore MDM può abilitare la modalità smarrito su un dispositivo supervisionato con iOS 9.3 o successivo. Quando è abilitata la modalità smarrito, l'utente attuale viene disconnesso e il dispositivo non può essere sbloccato. Sullo schermo viene visualizzato un messaggio, personalizzabile dall'amministratore, che può contenere ad esempio un numero di telefono da chiamare nel caso in cui il dispositivo sia stato smarrito. Quando per un dispositivo viene attivata la modalità smarrito, l'amministratore può richiedere al dispositivo di inviare la propria posizione attuale e, facoltativamente, di emettere un suono. Quando un amministratore disattiva la modalità smarrito, unico caso in cui l'opzione può essere disattivata, l'utente ne viene informato tramite un messaggio nel blocco schermo o un avviso sullo schermata Home.

Blocco attivazione

Quando “Trova il mio iPhone” è attivato, il dispositivo non può essere riattivato se non vengono inserite le credenziali dell'ID Apple del proprietario o il codice precedente del dispositivo.

Con i dispositivi di proprietà di un'organizzazione, è consigliabile supervisionare i dispositivi, in modo tale che il blocco dell'attivazione possa essere gestito dall'organizzazione piuttosto che richiedere l'inserimento delle credenziali dell'ID Apple da parte dell'utente individuale per riattivare i dispositivi.

Sui dispositivi supervisionati, una soluzione MDM compatibile potrà archiviare un codice di bypass da utilizzare per eliminare automaticamente il blocco dell'attivazione nel caso in cui il dispositivo debba essere inizializzato e assegnato a un nuovo utente.

Di default, sui dispositivi supervisionati il blocco dell'attivazione non è mai abilitato, nemmeno se l'utente attiva “Trova il mio iPhone”. Tuttavia, una soluzione MDM può ricevere un codice di bypass e consentire l'abilitazione del blocco dell'attivazione sul dispositivo. Se Trova il mio iPhone è attivo quando la soluzione MDM abilita il blocco dell'attivazione, questo verrà abilitato in quel momento. Altrimenti, il blocco attivazione verrà abilitato non appena l'utente attiverà “Trova il mio iPhone”.

Per i dispositivi utilizzati in contesti educativi con un ID Apple gestito creato mediante Apple School Manager, il blocco attivazione può essere associato a un ID Apple di amministratore invece che a un ID Apple utente, oppure può essere disabilitato tramite il codice di bypass del dispositivo.

Tempo di utilizzo

“Tempo di utilizzo” è una funzionalità di iOS 12 che consente agli utenti di capire e controllare il proprio utilizzo di app e pagine web o quello dei propri figli. Gli utenti possono:

- Visualizzare i dati di utilizzo.
- Impostare limitazioni per l'uso delle app o del web.
- Configurare pause di utilizzo.
- Stabilire restrizioni aggiuntive.

Per un utente che gestisce l'utilizzo del proprio dispositivo, i controlli e i dati di utilizzo di “Tempo di utilizzo” possono essere sincronizzati tra i dispositivi associati allo stesso account di iCloud tramite la codifica end-to-end di CloudKit. Per questo è necessario che sull'account dell'utente sia abilitata l'autenticazione a due fattori (di default la sincronizzazione non è attiva). “Tempo di utilizzo” sostituisce la funzionalità Restrizioni delle versioni precedenti di iOS.

Quando un utente cancella la cronologia di Safari o elimina un'app, i dati di utilizzo corrispondenti vengono rimossi dal dispositivo e da tutti quelli sincronizzati.

Genitori e “Tempo di utilizzo”

I genitori possono utilizzare “Tempo di utilizzo” sui dispositivi iOS anche per capire e controllare l'utilizzo da parte dei figli. Se il genitore è l'organizzatore di una famiglia (in “In famiglia” di iCloud), può visualizzare i dati di utilizzo e gestire le impostazioni di “Tempo di utilizzo” per i propri figli. I figli vengono informati del fatto che i genitori hanno attivato “Tempo di utilizzo” e possono monitorare il proprio utilizzo anche personalmente. Quando i genitori attivano “Tempo di utilizzo” per i figli, impostano un codice che impedisce ai figli di effettuare modifiche. Al compimento dei diciotto anni (a seconda del paese o della regione) i figli possono disattivare il monitoraggio.

I dati di utilizzo e le impostazioni di configurazione vengono trasferite tra i dispositivi dei genitori e dei figli tramite una connessione con codifica end-to-end al sevizio di identificazione Apple (IDS). I dati codificati potrebbero essere brevemente archiviati sui server di IDS finché non vengono letti dal dispositivo ricevente (ad esempio, appena iPhone o iPad vengono accesi, se erano spenti). I dati non possono essere letti da Apple.

Analisi di “Tempo di utilizzo”

Se l'utente attiva “Condividi dati iPhone e Watch”, solo i seguenti dati resi anonimi vengono raccolti, in modo che Apple possa capire in che modo viene usato “Tempo di utilizzo”.

- Se “Tempo di utilizzo” è stato attivato durante Impostazione Assistita o in seguito in Impostazioni.
- Se “Tempo di utilizzo” è attivato.
- Se è abilitata una pausa di utilizzo.
- Il numero di volte che “Richiedi più tempo” è stato utilizzato.
- Numero di limitazioni per le app.

Apple non raccoglie nessun dato specifico sulle app e sul web. Quando un utente visualizza un elenco di app nelle informazioni di utilizzo di “Tempo di utilizzo”, le icone delle app vengono prelevate direttamente da App Store, che non conserva nessun dato da questa richiesta.

Controlli per la privacy

Apple prende molto seriamente la privacy dei clienti, per questo ha integrato in iOS numerosi controlli e opzioni che permettono agli utenti di decidere come e quando le app possono utilizzare le loro informazioni, nonché quali informazioni vengono utilizzate.

Servizi di localizzazione

I servizi di localizzazione utilizzano il GPS, il Bluetooth e informazioni crowd-sourced sulle posizioni degli hotspot Wi-Fi e delle antenne cellulari per determinare la posizione approssimativa dell'utente. È possibile disattivare i servizi di localizzazione con un unico interruttore in Impostazioni, oppure l'utente può approvare l'accesso per le singole app che li utilizzano, scegliendo inoltre se le app possono richiedere dati sulla posizione solo quando sono in uso o sempre. Gli utenti possono decidere di non consentire l'accesso e modificare la propria scelta in qualsiasi momento in Impostazioni. Da Impostazioni è possibile impostare l'accesso su "sempre", "quando in uso" o su "mai", a seconda di come verrà utilizzata la posizione richiesta dall'app. In più, se le app a cui è consentito l'accesso alla posizione in qualsiasi momento utilizzano il servizio quando sono in background, un messaggio avvisa l'utente, che può quindi scegliere di modificare l'impostazione.

Gli utenti possono inoltre controllare con precisione l'utilizzo delle informazioni sulla posizione da parte dei servizi di sistema. Ad esempio, è possibile disattivare l'inclusione della posizione nelle informazioni raccolte dai servizi di analisi utilizzate da Apple per migliorare iOS, le informazioni di Siri basate sulla posizione, il contesto basato sulla posizione per le ricerche dei suggerimenti di Siri, le condizioni locali del traffico e le posizioni rilevanti visitate in passato.

Accesso ai dati personali

iOS impedisce alle app di accedere senza permesso alle informazioni personali dell'utente. Inoltre, da Impostazioni gli utenti possono vedere l'elenco delle app a cui hanno consentito l'accesso a certe informazioni, nonché concedere o revocare l'autorizzazione. Ciò include l'accesso a:

- Contatti
- Calendari
- Promemoria
- Foto
- Movimento e fitness
- Localizzazione
- Apple Music
- L'attività relativa a musica e video
- Microfono
- Fotocamera
- HomeKit
- Salute
- Riconoscimento vocale
- Condivisione Bluetooth
- Libreria multimediale

Se l'utente accede a iCloud, le app avranno accesso di default a iCloud Drive. L'utente può controllare l'accesso di ciascuna app nella sezione iCloud di Impostazioni. iOS fornisce inoltre delle restrizioni che impediscono lo spostamento di dati tra le app e gli account installati dalla soluzione MDM e quelli installati dall'utente.

Politica di tutela della privacy

Per consultare la politica di tutela della privacy di Apple, vai su: https://www.apple.com/it/legal/privacy

Certificazioni e programmi di sicurezza

Nota: per le ultime informazioni sulle certificazioni di sicurezza di iOS, sulle convalide e per linee guida sull'argomento, consulta: https://support.apple.com/HT202739

Certificazioni ISO 27001 e 27018

Apple ha ricevuto le certificazioni ISO 27001 e 27018 per il sistema di gestione della sicurezza delle informazioni per l'infrastruttura, lo sviluppo e le operazioni che supportano i seguenti prodotti e servizi: Apple School Manager, iTunes U, iCloud, iMessage, FaceTime, ID Apple gestiti, Siri e Schoolwork, in accordo con la Dichiarazione di applicabilità 2.1 dell'11 luglio 2017. La conformità di Apple agli standard ISO è stata certificata dalla British Standards Institution. I certificati di conformità per gli standard ISO 27001 e ISO 27018 sono disponibili sul sito web della BSI. Per consultare i certificati, vai su:

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

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

Convalida della codifica (FIPS 140-2)

I moduli di codifica presenti in iOS sono stati sottoposti ripetutamente al processo di convalida in conformità allo standard FIPS (U.S. Federal Information Processing Standards) 140-2 a partire da iOS 6 e versioni successive. Come per ogni release principale, Apple invia i moduli a CMVP perché vengano nuovamente convalidati quando viene lanciato il sistema operativo iOS. Il programma convalida l'integrità delle operazioni di codifica delle app di Apple e di terze parti che utilizzano correttamente i servizi di codifica di iOS e gli algoritmi approvati.

Apple ha ricevuto la convalida FIPS 140-2 per il modulo hardware integrato identificato come **Apple Secure Enclave Processor (SEP) Secure Key Store (SKS) Cryptographic Module** che abilita all'utilizzo delle chiavi generate e gestite dal processore Secure Enclave. Apple continuerà a perseguire i più alti livelli per i moduli hardware con ogni successiva versione di iOS.

Certificazione Common Criteria (ISO 15408)

Fin dal lancio di iOS 9, Apple ha ottenuto certificazioni ISO per ogni principale release secondo il programma Common Criteria Certification e ha esteso la copertura per includere:

- Profilo di protezione fondamentale per i dispositivi mobili
  - Pacchetto esteso per gli agenti di gestione dei dispositivi mobili
  - Pacchetto esteso per i client LAN wireless
  - Modulo PP per il client VPN
- Profilo di protezione per il software applicativo
  - Pacchetto esteso per i browser web

Si prevede che iOS 12 includa certificati aggiuntivi per:

- Pacchetto esteso per i client e-mail

Apple ha in programma di estendere la copertura con ogni successiva versione di iOS.

All'interno della comunità tecnologica internazionale, Apple partecipa attivamente allo sviluppo di profili di protezione collaborativi attualmente non disponibili incentrati sulla valutazione di tecnologie fondamentali per la sicurezza mobile. Inoltre, Apple continua a valutare e a richiedere certificazioni per le versioni nuove e aggiornate dei profili di protezione collaborativi già disponibili e in fase di sviluppo.

Programma Commercial Solutions for Classified (CSfC)

Dove applicabile, Apple ha anche richiesto l'inclusione della piattaforma iOS e di vari servizi nell'elenco dei componenti del programma CSfC. Man mano che le piattaforme e i servizi Apple vengono sottoposti alle certificazioni Common Criteria, ne viene richiesta anche l'inclusione nell'elenco del programma CSfC.

Per visualizzare i componenti aggiunti più di recente, consulta: https://www.nsa.gov/resources/everyone/csfc/components-list/

Guide alla configurazione della sicurezza

Apple ha collaborato con governi di tutto il mondo per sviluppare guide che forniscano istruzioni e consigli per mantenere un ambiente più sicuro per i dispositivi nelle situazioni di alto rischio. Tali guide offrono informazioni precise e verificate su come configurare e utilizzare le funzionalità integrate di iOS per ottenere una maggiore sicurezza.

Programma di bug bounty sulla sicurezza di Apple

Apple ricompensa coloro che trovano e condividono con Apple delle falle importanti nella sicurezza. Perché le segnalazioni siano considerate idonee per un programma di bug bounty di Apple, devono includere un resoconto chiaro ed essere corredate da un PoC (Proof of Concept) funzionante. La vulnerabilità deve avere effetto sull'ultima versione di iOS e, quando rilevante, sull'hardware più recente. L'importo esatto del pagamento verrà determinato da Apple una volta verificata la segnalazione. I criteri includono la novità, la probabilità di esposizione e il grado di interazione richiesta da parte dell'utente.

Dopo che i problemi rilevati sono stati adeguatamente condivisi, per Apple diventa prioritaria la risoluzione, quanto prima, delle falle confermate. Quando pertinente, Apple riconoscerà l'esistenza di tali falle pubblicamente, salvo diversa richiesta.

Categoria	Compenso massimo (USD)
Componenti del firmware di avvio sicuro	200.000 USD
Estrazione di materiale confidenziale protetto da Secure Enclave	100.000 USD
Esecuzione di codice arbitrario con privilegi kernel	50.000 USD
Accesso non autorizzato ai dati dell'account di iCloud sui server di Apple	50.000 USD
Accesso da un processo sandboxed ai dati dell'utente al di fuori della sandbox	25.000 USD

Conclusione

Il nostro impegno per la sicurezza

Apple si impegna a proteggere i propri clienti con tecnologie evolute per la privacy e la sicurezza progettate per tutelare le informazioni personali, nonché adottando soluzioni a tutto tondo per contribuire a salvaguardare i dati aziendali in un ambiente enterprise.

La sicurezza è integrata in iOS. Dalla piattaforma fino alle reti e alle app, iOS include tutto quello di cui un'azienda ha bisogno. Insieme, questi componenti permettono a iOS di offrire una sicurezza leader nel settore senza compromettere l'esperienza utente.

Apple utilizza un'infrastruttura di sicurezza integrata e omogenea in iOS e nell'ecosistema di app per iOS. La codifica dello spazio di archiviazione basata su hardware fornisce funzionalità di inizializzazione a distanza in caso di smarrimento del dispositivo e permette agli utenti di rimuovere completamente tutte le informazioni aziendali e personali quando il dispositivo viene venduto o trasferito a un'altra persona. Inoltre, le informazioni diagnostiche sono raccolte in maniera anonima.

Le app per iOS sviluppate da Apple sono progettate con l'obiettivo di garantire la massima sicurezza. Ad esempio, iMessage e FaceTime forniscono una codifica client-to-client. Per le app di terze parti, la firma obbligatoria del codice, il sandboxing e le autorizzazioni forniscono agli utenti una protezione secondo gli standard industriali contro virus, malware e altri attacchi. Il processo di invio delle app ad App Store contribuisce a tutelare ulteriormente gli utenti da questi rischi; infatti, tutte le app per iOS sono sottoposte a verifica prima di essere rese disponibili.

Consigliamo vivamente alle aziende di valutare le proprie politiche in materia di IT e sicurezza per avere la certezza di utilizzare appieno tutte le tecnologie di protezione integrate in iOS.

Apple dispone di un team dedicato in grado di offrire assistenza per tutte le problematiche di sicurezza riferite ai prodotti Apple. Il team fornisce servizi di auditing e testing non solo per i prodotti in fase di sviluppo, ma anche per quelli già rilasciati. Fornisce inoltre strumenti di sicurezza e training specifico, oltre a monitorare le segnalazioni di nuove minacce e problemi relativi alla sicurezza. In più, Apple fa parte del Forum of Incident Response and Security Teams (FIRST).

Per maggiori informazioni su come segnalare eventuali problemi ad Apple e per iscriverti alle notifiche di sicurezza, vai su: https://www.apple.com/it/support/security/

Glossario

Address space layout randomization (ASLR)	Una tecnica adottata da iOS per rendere la riuscita di un attacco da parte di un bug software molto più difficile. Dato che gli indirizzi e gli offset della memoria sono imprevedibili, questi valori non possono essere fissati nel codice di exploit. In iOS 5 o versione successiva, la posizione di tutte le app e le librerie di sistema è casuale, inoltre tutte le app di terze parti devono essere compilate come PIE (Position Independent Executable).
bit seed del software	Bit dedicati nel motore AES di Secure Enclave che vengono applicati all'UID quando vengono generate chiavi da quest'ultimo. Ogni bit seed del software ha dei bit di blocco corrispondenti. La ROM di avvio di Secure Enclave e il sistema operativo possono modificare indipendentemente il valore di ogni bit seed del software solo se il bit di blocco corrispondente non è stato impostato. Una volta che il bit di blocco è stato impostato, non è possibile modificare né il bit seed del software né il bit di blocco. I bit seed del software e i rispettivi blocchi vengono ripristinati quando Secure Enclave si riavvia.
Boot ROM	Il primo codice eseguito dal processore di un dispositivo al momento dell'avvio. In quanto parte integrante del processore, non può essere alterato né da Apple né da un malintenzionato.
chiave del file system	La chiave che codifica i metadati di ciascun file, inclusa la relativa chiave di classe. È conservata nella Effaceable Storage per consentire un'inizializzazione veloce più che per garantirne la riservatezza.
chiave per file	La chiave AES a 256 bit utilizzata per codificare un file nel file system. La chiave per file è cifrata da una chiave di classe e archiviata nei metadati del file.
cifratura della chiave	Codificare una chiave con un'altra. iOS utilizza l'algoritmo di cifratura chiavi NIST AES, come da RFC 3394.
Circuito integrato (Integrated Circuit, IC)	Detto anche microchip.
controller della memoria	La chiave AES a 256 bit utilizzata per codificare un file nel file system. La chiave per file è cifrata da una chiave di classe e archiviata nei metadati del file.
derivazione	Il processo tramite il quale il codice di un utente viene trasformato in una chiave crittografica e rinforzato con l'UID del dispositivo. Questo fa sì che un eventuale attacco al dispositivo debba essere di forza bruta, quindi limitato per numero di tentativi possibili e non eseguibile in parallelo. L'algoritmo di derivazione è PBKDF2, che utilizza la codifica AES basata sull'UID del dispositivo come funzione pseudo casuale per ciascuna iterazione.
Device Firmware Upgrade (DFU)	Una modalità in cui il codice Boot ROM del dispositivo attende di essere recuperato via USB. Lo schermo è nero, ma alla connessione con un computer su cui è installato iTunes compare il seguente messaggio: “iTunes ha rilevato un iPad in modalità di recupero. Devi ripristinare iPad prima di usarlo con iTunes”.
ECDSA	Un algoritmo di firma digitale basato sulla codifica su curve ellittiche.
Effaceable Storage	Un'area dedicata dell'archiviazione NAND utilizzata per memorizzare chiavi di codifica; può essere interrogata direttamente e cancellata in maniera sicura. Anche se non costituisce una protezione quando il malintenzionato è materialmente in possesso del dispositivo, le chiavi conservate nella Effaceable Storage possono essere utilizzate nell'ambito di una gerarchia di chiavi per consentire un'inizializzazione veloce e aumentare così la sicurezza.
group ID (GID)	Come l'UID, ma comune a tutti i processori all'interno di una classe.

iBoot	Codice che carica XNU nell'ambito della procedura di avvio sicura. A seconda della generazione del chip integrato, iBoot può essere caricato da LLB o direttamente dalla ROM di avvio.
Identificatore unico del processore (ECID)	Un identificatore a 64 bit specifico per il processore in ciascun dispositivo iOS. Quando l'utente risponde a una chiamata su uno dei dispositivi, i dispositivi nelle vicinanze abbinati tramite iCloud smetteranno di suonare dopo una breve trasmissione via Bluetooth Low Energy 4.0. I byte di tale notifica sono codificati con lo stesso metodo con cui vengono annunciati i trasferimenti di Handoff. È utilizzato durante il processo di personalizzazione e non è considerato segreto.
ID univoco (UID)	Una chiave AES a 256 bit impressa in ciascun processore nella fase di fabbricazione. Non può essere letta dal firmware o dal software ed è utilizzata solo dal motore AES hardware del processore. Per ottenere la chiave effettiva, un malintenzionato dovrebbe sferrare un attacco fisico altamente sofisticato e costoso contro il chip del processore. L'UID non è collegato a nessun altro identificatore sul dispositivo, nemmeno all'UDID.
Joint Test Action Group (JTAG)	Uno strumento standard per il debug dell'hardware utilizzato dai programmatori e dagli sviluppatori di circuiti.
keybag	Una struttura dati utilizzata per conservare una raccolta di chiavi di classe. Ogni tipo (Utente, Dispositivo, Sistema, Backup, Escrow o Backup iCloud) ha lo stesso formato, ossia: • Un'intestazione contenente: – Versione (impostata su 3 in iOS 5). – Tipo (Sistema, Backup, Escrow o Backup iCloud). – UUID della keybag. – Un codice HMAC se la keybag è firmata. – Il metodo utilizzato per cifrare le chiavi della classe: di cifratura con l'UID o con PBKDF2, insieme al salt e al numero delle iterazioni. • Un elenco delle chiavi di classe: – UUID della chiave. – Classe (la classe di protezione dati per file o portachiavi). – tipo di cifratura (solo chiave derivata dall'UID; chiave derivata dall'UID e chiave derivata dal codice) – Chiave di classe cifrata. – Chiave pubblica per le classi asimmetriche.
Low-Level Bootloader (LLB)	Sui sistemi con un'architettura di avvio a due fasi, codice invocato dalla ROM di avvio e che a sua volta carica iBoot nell'ambito della procedura di avvio sicura.
mappatura angolare del disegno papillare	Una rappresentazione matematica della direzione e dell'ampiezza delle creste estrapolate da una porzione di impronta digitale.
modulo di sicurezza hardware (Hardware Security Module, HSM)	Un computer specializzato anti-manomissione che protegge e gestisce le chiavi digitali.
Portachiavi	Infrastruttura e set di API utilizzati da iOS e dalle app di terze parti per archiviare e recuperare password, chiavi e altre credenziali sensibili.
Profilo di provisioning	Un file plist firmato da Apple contenente un set di entità e autorizzazioni che permettono di installare e testare app su un dispositivo iOS. Un profilo di provisioning di sviluppo elenca i dispositivi scelti dallo sviluppatore per la distribuzione personalizzata, mentre il profilo di provisioning di distribuzione contiene l'ID di un'app sviluppata dall'azienda.
Protezione dei dati	Meccanismo di protezione dei file e del portachiavi per iOS. Può anche riferirsi alle API utilizzate dalle app per proteggere i file e gli elementi del portachiavi.
Protezione dell'integrità dei coprocessori di sistema (SCIP)	I coprocessori di sistema sono CPU sullo stesso SoC del processore per le applicazioni.

Registro di avanzamento dell'avvio (BPR)	Un insieme di marcatori hardware del chip integrato che il software può utilizzare per tenere traccia delle modalità di avvio intraprese dal dispositivo, come la modalità DFU o la modalità di recupero. Una volta che un marcatore del registro di avanzamento dell'avvio è impostato, non può essere eliminato. Questo consente al software successivo di ottenere un indicatore attendibile dello stato del sistema.
Scambio su curve ellittiche Diffie-Hellman (ECDHE)	Scambio su curve ellittiche Diffie-Hellman con chiavi effimere. ECDHE consente a due parti di accordarsi su una chiave segreta in un modo che impedisce alla chiave di essere scoperta da un soggetto che intercetta i messaggi scambiati dalle due parti.
Servizio Apple Push Notification (APN)	Un servizio fornito da Apple che trasmette notifiche push ai dispositivi iOS in tutto il mondo.
Servizio di identificazione di Apple (IDS)	La directory Apple contente le chiavi pubbliche di iMessage, gli indirizzi APN nonché i numeri di telefono e gli indirizzi e-mail utilizzati per cercare le chiavi e gli indirizzi dei dispositivi.
system on a chip (SoC)	Un circuito integrato (IC) che riunisce vari componenti su un singolo chip. Il processore per le applicazioni, Secure Enclave e altri coprocessori sono componenti del SoC.
Uniform Resource Identifier (URI)	Una stringa di caratteri che identifica una risorsa web.
XNU	Il kernel alla base dei sistemi operativi iOS e macOS. È considerato attendibile e applica misure di sicurezza come la firma del codice, il sandboxing, la verifica delle autorizzazioni e la ASLR.

Cronologia delle revisioni del documento

Data	Riepilogo
Novembre 2018	**Aggiornato per iOS 12.1** • Chiamate FaceTime di gruppo
Settembre 2018	**Aggiornato per iOS 12** • Secure Enclave • Protezione dell'integrità del sistema operativo • Modalità rapida delle carte in modalità “Basso consumo” • Modalità DFU e di recupero • Telecomandi TV HomeKit • Biglietti contactless • Tessere identificative studente • Suggerimenti di Siri • Abbreviazioni in Siri • App Comandi Rapidi • Gestione delle password dell'utente • Tempo di utilizzo • Certificazioni e programmi di sicurezza
Luglio 2018	**Aggiornato per iOS 11.4** • Politiche per le rilevazioni biometriche • HomeKit • Apple Pay • Chat con l'azienda • Messaggi su iCloud • Apple Business Manager
Dicembre 2017	**Aggiornato per iOS 11.2** • Apple Pay Cash **Aggiornato per iOS 11.1** • Certificazioni e programmi di sicurezza • Touch ID/Face ID • Note condivise • Codifica end-to-end di CloudKit • TLS • Apple Pay, pagare tramite Apple Pay sul web • Suggerimenti di Siri • iPad condiviso Per ulteriori informazioni sul contenuto di sicurezza di iOS 11, consulta: https://support.apple.com/HT208112

Data	Riepilogo
Luglio 2017	**Aggiornato per iOS 10.3** • System Enclave • Protezione dati dei file • Keybag • Certificazioni e programmi di sicurezza • SiriKit • HealthKit • Sicurezza della rete • Bluetooth • iPad condiviso • Modalità smarrito • Blocco attivazione • Controlli per la privacy Per ulteriori informazioni sul contenuto di sicurezza di iOS 10.3, consulta: https://support.apple.com/HT207617
Marzo 2017	**Aggiornato per iOS 10** • Sicurezza del sistema • Classi di protezione dati • Certificazioni e programmi di sicurezza • HomeKit, ReplayKit, SiriKit • Apple Watch • Wi-Fi, VPN • Single Sign-on • Apple Pay, pagare tramite Apple Pay sul web • Aggiunta di carte di credito, di debito e prepagate • Suggerimenti di Safari Per ulteriori informazioni sul contenuto di sicurezza di iOS 10, consulta: http://support.apple.com/HT207143
Maggio 2016	**Aggiornato per iOS 9.3** • ID Apple gestito • Autenticazione a due fattori per ID Apple • Keybag • Certificazioni di sicurezza • Modalità smarrito, blocco attivazione • Protezione note • Apple School Manager, iPad condiviso Per ulteriori informazioni sul contenuto di sicurezza di iOS 9.3, consulta: https://support.apple.com/HT206166

Data	Riepilogo
Settembre 2015	**Aggiornato per iOS 9** • Blocco attivazione di Apple Watch • Politiche per il codice • Supporto per l'API di Touch ID • La protezione dati su A8 utilizza AES-XTS • Keybag per aggiornamenti software automatici • Aggiornamenti delle certificazioni • Modello di attendibilità delle app aziendali • Protezione dati per i segnalibri di Safari • Sicurezza dei trasferimenti delle app • Specifiche VPN • Accesso remoto via iCloud per HomeKit • Carte fedeltà di Apple Pay, app dell'ente di emissione della carta di Apple Pay • Indicizzazione sul dispositivo di Spotlight • Modello di abbinamento di iOS • Apple Configurator 2 • Restrizioni Per ulteriori informazioni sul contenuto di sicurezza di iOS 9, consulta: https://support.apple.com/HT205212

Novembre 2018