Seguridad de iOS

iOS 11

Enero de 2018

Contenido

Página 4 **Introducción**

Página 6 **Seguridad del sistema**
Cadena de arranque seguro
Autorización de software del sistema
Secure Enclave
Touch ID
Face ID

Página 14 **Encriptación y protección de datos**
Funciones de seguridad de hardware
Protección de datos de archivo
Códigos
Clases de protección de datos
Protección de datos del llavero
Acceso a contraseñas guardadas en Safari
Depósitos de claves
Certificaciones de seguridad y programas

Página 26 **Seguridad de las apps**
Firma de código de apps
Seguridad del proceso de ejecución
Extensiones
Grupos de apps
Protección de datos en apps
Accesorios
HomeKit
SiriKit
HealthKit
ReplayKit
Notas seguras
Notas compartidas
Apple Watch

Página 41 **Seguridad de la red**
TLS
VPN
Wi-Fi
Bluetooth
Inicio de sesión único (SSO)
Seguridad de AirDrop
Compartir contraseña de Wi-Fi

Página 47 **Apple Pay**
Componentes de Apple Pay
Cómo Apple Pay usa el componente Secure Element
Cómo Apple Pay usa el controlador NFC
Datos de tarjetas de crédito, débito y prepago
Autorización de pagos

Código de seguridad dinámico específico para cada transacción
Pagos sin contacto con Apple Pay
Pagos con Apple Pay desde apps
Pagos con Apple Pay en la web o con Handoff
Tarjetas de recompensa
Apple Pay Cash
Tarjetas Suica
Suspensión, eliminación y borrado de tarjetas

Página 59 **Servicios de Internet**
Apple ID
iMessage
FaceTime
iCloud
Llavero de iCloud
Siri
Continuidad
Sugerencias de Safari, Sugerencias de Siri, Consultar, #images, app News, y widget de News en países sin News

Página 77 **Controles de dispositivos**
Protección mediante código
Modelo de enlace de iOS
Aplicación de la configuración
Mobile Device Management (MDM)
iPad compartido
Apple School Manager
Inscripción de dispositivos
Apple Configurator 2
Supervisión
Restricciones
Borrado remoto
Modo perdido
Bloqueo de activación

Página 85 **Controles de privacidad**
Localización
Acceso a datos personales
Política de privacidad

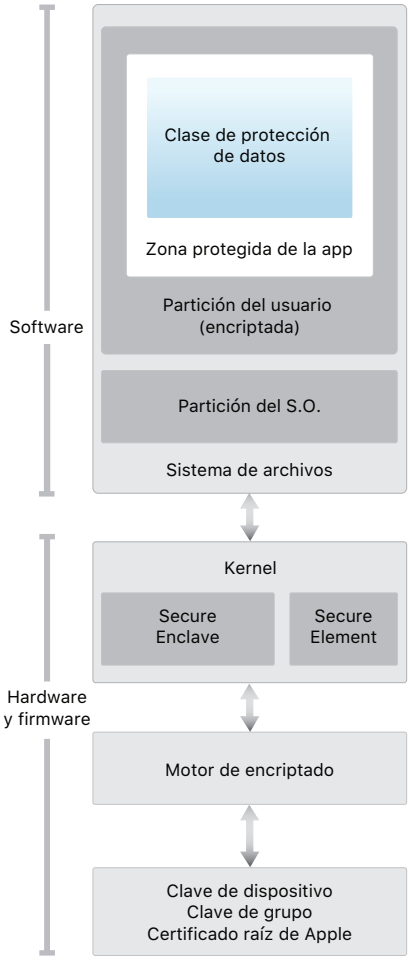
Página 87 **Recompensas de seguridad de Apple**

Página 88 **Conclusión**
Compromiso con la seguridad

Página 89 **Glosario**

Página 91 **Historial de revisión del documento**

Introducción



El diagrama de la arquitectura de seguridad de iOS proporciona una visión general de las diferentes tecnologías comentadas en este documento.

Apple diseñó la plataforma iOS en torno a la seguridad. Cuando nos dispusimos a crear la mejor plataforma móvil posible, aprovechamos nuestra vasta experiencia para construir una arquitectura completamente nueva. Pensamos en los riesgos de seguridad del entorno del escritorio y definimos un enfoque nuevo de seguridad para el diseño de iOS. Desarrollamos e incorporamos funciones innovadoras que refuerzan la seguridad del entorno móvil y protegen todo el sistema. Esto hace que iOS constituya un gran avance en el ámbito de la seguridad para dispositivos móviles.

Todos los dispositivos iOS combinan software, hardware y servicios que se han diseñado para funcionar en conjunto con el fin de proporcionar la máxima seguridad y una experiencia de usuario transparente. iOS protege el dispositivo y los datos que este contiene, así como el ecosistema en su totalidad, incluidas todas las acciones que los usuarios realizan de forma local, en redes y con servicios clave de Internet.

El sistema operativo iOS y los dispositivos iOS proporcionan funciones de seguridad avanzadas y, además, son fáciles de usar. Muchas de estas funciones están activadas de forma predeterminada, por lo que los departamentos de TI no tienen que realizar extensas configuraciones. Además, las funciones de seguridad clave (como la encriptación de los dispositivos) no se pueden configurar; por lo que los usuarios no las pueden desactivar por error. Otras funciones, como Face ID, mejoran la experiencia del usuario al facilitar la protección del dispositivo y hacerla más intuitiva.

En este documento se proporciona información detallada sobre la implementación de la tecnología y las funciones de seguridad en la plataforma iOS. También resulta de utilidad a organizaciones que quieran combinar la tecnología y las funciones de seguridad de la plataforma iOS con sus propias políticas y procedimientos con el fin de satisfacer sus necesidades de seguridad específicas.

Este documento se divide en los temas siguientes:

- **Seguridad del sistema:** el software y hardware integrados y seguros que constituyen la plataforma para iPhone, iPad y iPod touch.
- **Encriptación y protección de datos:** la arquitectura y el diseño que se encargan de proteger los datos del usuario en caso de pérdida o robo del dispositivo, o si una persona no autorizada intenta utilizarlo o modificarlo.
- **Seguridad de las apps:** los sistemas que permiten la ejecución segura de las apps, sin poner en peligro la integridad de la plataforma.
- **Seguridad de la red:** los protocolos de red estándar del sector que proporcionan la autenticación segura y la encriptación de los datos durante la transmisión.
- **Apple Pay:** la implementación de Apple para realizar pagos seguros.

- **Servicios de Internet:** la infraestructura basada en la red de Apple para los servicios de mensajería, sincronización y respaldos.
- **Controles de dispositivos:** los métodos que permiten administrar dispositivos iOS, prevenir el uso no autorizado de los mismos o activar el borrado remoto en caso de pérdida o robo.
- **Controles de privacidad:** las funcionalidades de iOS que se pueden utilizar para controlar el acceso a la función de localización y a los datos de usuario.

Seguridad del sistema

Entrar al modo de actualización del firmware del dispositivo (DFU) Restaurar un dispositivo una vez que entra en modo DFU hace que vuelva a un estado anterior en buenas condiciones con la certeza de que contiene sólo el contenido firmado por Apple que no ha sido modificado. Se puede entrar al modo DFU manualmente.

Primero conecta el dispositivo a una computadora utilizando un cable USB.

Después:

En el iPhone X, iPhone 8 o iPhone 8 Plus, presiona y suelta rápidamente el botón para subir el volumen. Presiona y suelta rápidamente el botón para bajar el volumen. Luego, mantén presionado el botón lateral hasta que veas la pantalla del modo de recuperación.

En el iPhone 7 o iPhone 7 Plus, mantén presionado el botón lateral y el botón para bajar el volumen al mismo tiempo. Mantenlos presionados hasta que veas la pantalla del modo de recuperación.

En el iPhone 6s y modelos anteriores, iPad o iPod touch, mantén presionados el botón de inicio y el botón superior (o lateral) al mismo tiempo. Mantenlos presionados hasta que veas la pantalla del modo de recuperación.

Nota: cuando el modo DFU está activo, no se muestra nada en la pantalla. Si aparece el logotipo de Apple, significa que se presionó el botón lateral o el botón de activación/reposo durante demasiado tiempo.

La seguridad del sistema está diseñada de modo que tanto el software como el hardware están protegidos en todos los componentes centrales de los dispositivos iOS. Esto incluye el proceso de arranque, las actualizaciones de software y el coprocesador Secure Enclave. Esta arquitectura es fundamental para la seguridad del sistema iOS y en ningún caso interfiere con el uso del dispositivo.

La estrecha integración del hardware, software y servicios en los dispositivos iOS garantiza que todos los componentes del sistema sean de confianza, al mismo tiempo que valida el sistema en su conjunto. Se analizan y aprueban todos los pasos —desde el arranque inicial hasta las actualizaciones de software iOS para apps de terceros— con el fin de garantizar que el hardware y el software funcionen juntos a la perfección y utilicen los recursos correctamente.

Cadena de arranque seguro

Todos los pasos del proceso de arranque contienen componentes firmados criptográficamente por Apple para garantizar su integridad y se llevan a cabo únicamente después de haber verificado la cadena de confianza. Esto incluye los gestores de arranque, el kernel, las extensiones del kernel y el firmware de banda base. Esta cadena de arranque seguro permite garantizar que no se manipulen los niveles más profundos del software.

Cuando se enciende un dispositivo iOS, el procesador de aplicaciones ejecuta inmediatamente el código de la memoria de sólo lectura (o ROM de arranque). Este código inmutable, también conocido como raíz de confianza de hardware, se establece durante la fabricación del chip y, de forma implícita, es de confianza. El código de la memoria ROM de arranque contiene la clave pública de la entidad emisora de certificados (CA) raíz de Apple, que se utiliza para verificar que los gestores de arranque iBoot tengan la firma de Apple antes de permitir que se carguen. Este es el primer paso de la cadena de confianza, en la que cada paso garantiza que el siguiente esté firmado por Apple. Cuando el iBoot termina sus operaciones, verifica y ejecuta el kernel de iOS. Para dispositivos con un procesador S1, A9 o anterior de la serie A, existe un gestor de arranque de bajo nivel (LLB) adicional que se carga y verifica con la ROM de arranque, que a su vez carga y verifica iBoot.

Si la ROM de arranque no logra cargar el gestor de arranque de bajo nivel (en dispositivos antiguos) o iBoot (en dispositivos recientes), el dispositivo entrará en modo DFU. Si ocurre una falla en el gestor de arranque de bajo nivel (LLB) o en iBoot, y no es posible cargar o verificar el siguiente paso, se interrumpe el arranque y se solicita al usuario que conecte el dispositivo a iTunes. A esto se le conoce como modo de recuperación. En cualquier caso, debe conectarse el dispositivo a iTunes mediante un cable USB y se debe restaurar la configuración original de fábrica.

En el caso de los dispositivos que disponen de acceso a datos celulares, el subsistema de banda base utiliza también un proceso propio similar para el arranque seguro con software firmado y claves verificadas por el procesador de banda base.

En el caso de los dispositivos que cuentan con Secure Enclave, el coprocesador Secure Enclave utiliza también un proceso de arranque seguro que garantiza la verificación y firma de su propio software por parte de Apple. Consulta la sección "Secure Enclave" de este documento.

Para obtener más información sobre cómo acceder manualmente al modo de recuperación, consulta: https://support.apple.com/es-lamr/HT1808.

Autorización de software del sistema

Apple lanza regularmente actualizaciones de software para solucionar los problemas de seguridad que van surgiendo y ofrecer nuevas características. Dichas actualizaciones se proporcionan de manera simultánea para todos los dispositivos compatibles. Los usuarios reciben notificaciones relativas a la actualización de iOS en su dispositivo y en iTunes. Las actualizaciones se proporcionan vía inalámbrica, para así facilitar la instalación de las correcciones de seguridad más recientes.

El proceso de arranque descrito anteriormente garantiza que sólo se pueda instalar código firmado por Apple en un dispositivo. Para evitar la instalación de versiones anteriores que no cuenten con las actualizaciones de seguridad más recientes, iOS utiliza un proceso conocido como *autorización de software del sistema*. Si fuera posible volver a una versión anterior, un atacante que tuviera un dispositivo podría instalar una versión más antigua de iOS para aprovechar alguna vulnerabilidad corregida en versiones más recientes.

En los dispositivos con Secure Enclave, el coprocesador Secure Enclave también utiliza el proceso de autorización de software del sistema para garantizar la integridad de su software y evitar la instalación de versiones anteriores. Consulta la sección "Secure Enclave" de este documento.

Las actualizaciones de software iOS se pueden instalar mediante iTunes o de forma inalámbrica (OTA) en el dispositivo. Con iTunes, se descarga e instala una copia completa de iOS. Las actualizaciones de software OTA sólo descargan los componentes necesarios para llevar a cabo la actualización en lugar de descargar todo el sistema operativo. De este modo, se mejora la eficiencia de la red. Asimismo, las actualizaciones de software se pueden almacenar en la memoria caché de una Mac con macOS High Sierra que tenga activada la función de almacenamiento de contenido en caché, de tal forma que los dispositivos iOS no tengan que volver a descargar de Internet la actualización necesaria. Sin embargo, aún será necesario ponerse en contacto con los servidores de Apple para completar el proceso de actualización.

Durante las actualizaciones de iOS, iTunes (o el propio dispositivo, en el caso de las actualizaciones de software OTA) se conecta al servidor de autorización de instalaciones de Apple y le envía una lista de medidas criptográficas para cada parte del paquete de instalación que se vaya a instalar (por ejemplo, iBoot, el kernel o una imagen del sistema operativo), un valor antirreproducción aleatorio (valor único) y el identificador único del dispositivo (ECID).

El servidor de autorización coteja la lista de medidas presentada con las versiones cuya instalación se permite y, si encuentra una coincidencia, agrega el ECID a la medida y firma el resultado. Como parte del proceso de actualización, el servidor envía un conjunto completo de datos firmados al dispositivo. Agregar ECID "personaliza" la autorización para el dispositivo

que realiza la solicitud. El servidor sólo autoriza y firma las medidas conocidas, de modo que se garantiza que la actualización se lleve a cabo de acuerdo con las especificaciones de Apple.

En la evaluación de la cadena de confianza realizada durante el arranque se verifica que la firma proceda de Apple y que la medida del elemento cargado desde el disco, combinada con el ECID del dispositivo, coincida con el contenido de lo firmado.

Estos pasos garantizan que la autorización sea para un dispositivo específico e impiden que una versión de iOS antigua se copie de un dispositivo a otro. El valor único impide que un atacante guarde la respuesta del servidor y la utilice para manipular un dispositivo o modificar el software del sistema de algún otro modo.

Secure Enclave

El Secure Enclave es un coprocesador incorporado en los procesadores Apple T1, Apple S2, Apple S3, Apple A7, o posteriores de la serie A. Utiliza memoria encriptada e incluye un generador de números aleatorios en hardware. El Secure Enclave proporciona todas las operaciones criptográficas para la administración de la clave de protección de datos y mantiene la integridad de la misma incluso si el kernel ha sido manipulado. La comunicación entre el Secure Enclave y el procesador de aplicaciones se aísla en un buzón dirigido por interruptores y búfers de datos de memoria compartida.

El Secure Enclave ejecuta una versión personalizada de Apple del microkernel L4. El microkernel está firmado por Apple, verificado como parte de la cadena de arranque seguro de iOS y actualizado mediante un proceso de actualización de software personalizado.

Cuando el dispositivo se enciende, se crea una clave efímera, vinculada al UID del dispositivo, que se utiliza para encriptar la parte que ocupa el Secure Enclave en el espacio de la memoria del dispositivo. La memoria del Secure Enclave también se autentica con la clave efímera, excepto en el procesador A7 de Apple. En el procesador A11 de Apple, se utiliza un árbol de integridad para evitar la reproducción de la memoria del Secure Enclave, que es crítica para la seguridad, y se encuentra autenticada por la clave efímera y los valores únicos almacenados en la SRAM integrada en el chip.

Además, se encriptan los datos que el Secure Enclave guarda en el sistema de archivos utilizando una clave vinculada al UID y un contador antirreproducciones. Los servicios antirreproducción del Secure Enclave se utilizan para revocar datos de eventos que marcan límites a la antirreproducción, entre los que se incluyen:

- Cambiar el código
- Activar/desactivar Touch ID o Face ID
- Agregar/eliminar huellas digitales
- Restablecer Face ID
- Agregar/eliminar tarjetas de Apple Pay
- Borrar todo el contenido y la configuración

El Secure Enclave también es responsable de procesar los datos faciales y de huellas digitales obtenidos mediante los sensores de Touch ID y Face ID con la finalidad de determinar si existe una coincidencia, en cuyo caso permitirá el acceso o las compras en nombre del usuario.

Touch ID

Touch ID es el sistema de detección de huellas digitales que hace posible acceder de forma segura al iPhone y iPad de forma más rápida y sencilla. Esta tecnología lee los datos de huella digital desde cualquier ángulo y almacena continuamente más información sobre la huella del usuario, ya que el sensor amplía el mapa de huella digital con cada uso a medida que identifica más nodos superpuestos.

Face ID

Con sólo una mirada, Face ID desbloquea de forma segura el iPhone X. Esta tecnología proporciona autenticación intuitiva y segura mediante el sistema de la cámara TrueDepth, el cual utiliza tecnologías avanzadas para registrar con precisión la geometría de tu cara. Face ID confirma la atención al detectar la dirección de tu mirada y a continuación utiliza redes neuronales para buscar una coincidencia y evitar el robo de identidad, de modo que puedas desbloquear tu teléfono con tan solo una mirada. Face ID se adapta automáticamente a los cambios en tu apariencia y protege cuidadosamente la privacidad y seguridad de tus datos biométricos.

Touch ID, Face ID y códigos

Para usar Touch ID o Face ID, debes configurar tu dispositivo para que se solicite un código al desbloquearlo. Cuando Touch ID o Face ID detectan una coincidencia, tu dispositivo se desbloquea sin solicitar el código del dispositivo. De este modo, los usuarios no tienen que ingresar el código muy a menudo y pueden utilizar uno más largo y complejo. Touch ID y Face ID no reemplazan tu código, sino que proporcionan acceso fácil a tu dispositivo dentro de unos límites y restricciones de tiempo razonables. Esto es importante, ya que un código seguro es la base de la protección criptográfica de tu dispositivo iOS.

Puedes usar tu código en lugar de Touch ID o Face ID cuando quieras, y es obligatorio en los casos siguientes:

- Cuando el dispositivo se acaba de encender o reiniciar.
- Cuando el dispositivo no se ha desbloqueado en las últimas 48 horas.
- Cuando no se ha usado el código para desbloquear el dispositivo en las últimas 156 horas (seis días y medio) y no se ha desbloqueado el dispositivo usando Face ID en las últimas cuatro horas.
- Cuando el dispositivo ha recibido un comando de bloqueo remoto.
- Después de cinco intentos fallidos de encontrar una coincidencia.
- Después de iniciar el apagado del dispositivo o una llamada Emergencia SOS.

Cuando Touch ID o Face ID están activados, el dispositivo se bloquea inmediatamente cuando se presiona el botón lateral, y cada que el dispositivo entra en modo de reposo. Touch ID y Face ID requieren una coincidencia (o, de forma opcional, el código) cada vez que se activa el dispositivo.

La probabilidad de que una persona al azar mire tu iPhone X y lo desbloquee usando Face ID es aproximadamente de 1 en 1,000,000 (frente al 1 en 50,000 de Touch ID). Como medida de protección adicional, tanto Touch ID como Face ID permiten sólo cinco intentos de coincidencia fallidos; después será necesario ingresar el código para obtener acceso al dispositivo. Con Face ID, la probabilidad de un error de reconocimiento varía en el caso de gemelos y hermanos que se parecen, así como en

niños menores de 13 años de edad, dado que aún no se han desarrollado por completo sus rasgos faciales característicos. Si te preocupa dicha posibilidad, Apple te recomienda utilizar un código como forma de autenticación.

Seguridad de Touch ID

El sensor de huellas digitales sólo se activa cuando el anillo de acero capacitivo que rodea el botón de inicio detecta el tacto de un dedo, lo cual activa la matriz de imágenes avanzada que escanea el dedo y envía la imagen obtenida al Secure Enclave. La comunicación entre el procesador y el sensor Touch ID se lleva a cabo a través de un bus de interfaz de periféricos en serie. El procesador envía los datos al Secure Enclave pero este no puede leerlos, ya que se encuentran encriptados y autenticados mediante una clave de sesión que se negocia utilizando una clave compartida proporcionada de fábrica para cada sensor Touch ID y su Secure Enclave correspondiente. La clave compartida es segura, aleatoria y diferente para cada sensor Touch ID. En el intercambio de claves de sesión, se utiliza la encapsulación de claves AES y ambas partes proporcionan una clave aleatoria que establece la clave de sesión y que utiliza la encriptación de transporte AES-CCM.

La imagen escaneada se almacena temporalmente en la memoria encriptada del Secure Enclave mientras se vectoriza para su análisis y, después, se descarta. El análisis utiliza la correspondencia de los ángulos del patrón de arrugas subdérmico. Este proceso es propenso a la pérdida de información y descarta los datos detallados que serían necesarios para reconstruir la huella real del usuario. El mapa de nodos resultante se almacena sin ninguna información de identidad en un formato encriptado que sólo el Secure Enclave puede leer, y nunca se envía a Apple ni se respalda en iCloud o iTunes.

Seguridad de Face ID

Face ID está diseñado para confirmar la atención del usuario, proporcionar funciones avanzadas de autenticación con un bajo índice de errores de coincidencia, y reducir el robo de identidad tanto físico como digital.

La cámara TrueDepth busca automáticamente tu cara cuando activas tu iPhone X al levantarlo o tocar la pantalla, así como cuando tu iPhone X intenta autenticar tu identidad para mostrar una notificación o cuando las apps compatibles solicitan autenticación mediante Face ID. Cuando se detecta una cara, Face ID confirma la atención e intenta desbloquear al detectar que tus ojos están abiertos y viendo hacia el dispositivo; para ofrecer mejor accesibilidad, esta función se desactiva cuando VoiceOver está activado y, opcionalmente, se puede desactivar por separado.

Una vez que se confirma la presencia de una cara que pone atención al dispositivo, la cámara TrueDepth proyecta y lee más de 30,000 puntos infrarrojos para formar un mapa de profundidad de la cara, junto con una imagen infrarroja en 2D. Estos datos se usan para crear una secuencia de imágenes en 2D y mapas de profundidad, los cuales se firman digitalmente y envían al Secure Enclave. Para contrarrestar el robo de identidad tanto digital como físico, la cámara TrueDepth aleatoriza la secuencia de imágenes en 2D y el mapa de profundidad, y proyecta un patrón aleatorio específico del dispositivo. Parte del motor neuronal del chip A11 Bionic, protegido dentro del Secure Enclave, trasforma estos datos en una representación matemática y la compara con los datos faciales registrados. Los datos faciales registrados son en sí una representación matemática de tu cara capturada a través de varias poses.

La coincidencia facial se realiza dentro del Secure Enclave utilizando redes neuronales programadas específicamente para tal propósito. Desarrollamos las redes neuronales de coincidencia facial utilizando más de mil millones de imágenes, incluyendo imágenes infrarrojas y de profundidad recopiladas en estudios realizados con el consentimiento informado de los participantes. Apple trabajó con participantes de todo el mundo para incluir un grupo de personas representativo, tomando en cuenta su género, edad, identidad étnica y otros factores. Se realizaron estudios adicionales según fuera necesario con la finalidad de ofrecer un alto grado de precisión a una gran diversidad de usuarios. Face ID está diseñado para funcionar con sombreros, bufandas, lentes, lentes de contacto y muchos lentes obscuros. Además, está diseñado para funcionar en interiores, exteriores e incluso en total oscuridad. Una red neuronal adicional programada para detectar y rechazar intentos de robo de identidad impide el desbloqueo de tu iPhone X mediante fotos o máscaras.

Los datos de Face ID, incluyendo las representaciones matemáticas de tu cara, están encriptados y sólo Secure Enclave puede acceder a ellos. Estos datos nunca salen de tu dispositivo. No se envían a Apple ni se incluyen en los respaldos del dispositivo. Los siguientes datos de Face ID se almacenan de forma encriptada sólo para uso exclusivo de Secure Enclave durante el funcionamiento normal:

- Las representaciones matemáticas de tu cara calculadas durante el registro.
- Las representaciones matemáticas de tu cara calculadas durante algunos intentos de desbloqueo cuando Face ID las considera útiles para mejorar las futuras verificaciones de coincidencias.

Las imágenes faciales capturadas durante el uso normal no se guardan, sino que se desechan inmediatamente una vez calculada la representación matemática ya sea para el registro o para la comparación con los datos de Face ID registrados.

Cómo Touch ID o Face ID desbloquean un dispositivo iOS

Si Touch ID o Face ID están desactivados, al momento en el que un dispositivo se bloquea, se descartan las claves de la clase de protección de datos más alta, las cuales se almacenan en el Secure Enclave. No se podrá acceder a los archivos y elementos del llavero de dicha clase hasta que se desbloquee el dispositivo con tu código.

Si tienes Touch ID o Face ID activados, cuando se bloquea el dispositivo, no se descartan las claves, sino que se encapsulan con una clave que se proporciona al subsistema de Touch ID o Face ID en el Secure Enclave. Durante un intento de desbloqueo de dispositivo, si el dispositivo encuentra una coincidencia, proporcionará la clave para desencapsular las claves de protección de datos, y el dispositivo se desbloqueará. Para desbloquear el dispositivo, el proceso proporciona protección adicional al solicitar la cooperación entre la protección de datos y los subsistemas de Touch ID y Face ID.

Cuando el dispositivo se reincia, se pierden las claves que Touch ID o Face ID requieren para desbloquear el dispositivo; ya que el Secure Enclave las descarta después de que se cumple cualquier condición que requiere la captura del código (por ejemplo, si pasan 48 horas sin desbloquear el dispositivo o si se realizan más de cinco intentos de coincidencia fallidos).

Para mejorar el rendimiento del desbloqueo y mantenerse al día con los cambios naturales en tu cara y apariencia, Face ID aumenta con el paso del tiempo las representaciones matemáticas que tiene almacenadas. Después de desbloquear el dispositivo, Face ID puede usar las representaciones matemáticas recién calculadas —si su calidad es suficiente— para un número finito de desbloqueos adicionales antes de descartar dichos datos. En cambio, si Face ID no logra reconocerte, pero la calidad de coincidencia es mayor que un límite específico e ingresas tu código inmediatamente después del intento fallido, Face ID toma otra captura y aumenta sus datos de Face ID registrados usando esa representación matemática recién calculada. Estos nuevos datos de Face ID se descartan si dejan de ser una coincidencia y después de un número finito de desbloqueos. Estos procesos de aumento permiten a Face ID reconocer cambios considerables de vello facial o uso de maquillaje y, a la vez, minimizar falsos positivos.

Touch ID, Face ID y ApplePay

También puedes usar Touch ID y Face ID con Apple Pay para realizar compras de manera fácil y rápida en tiendas, apps y en Internet. Para obtener más información sobre Touch ID y Apple Pay, consulta la sección Apple Pay de este documento.

Para autorizar una compra dentro de una app con Face ID, primero debes presionar el botón lateral dos veces para confirmar que quieres realizar el pago. A continuación debes autenticarte con Face ID y después colocar tu iPhone X cerca del lector de tarjetas inalámbrico. Si quieres seleccionar otro método de pago de Apple Pay después de la autenticación con Face ID, deberás volver a autenticarte, mas no tendrás que volver a presionar dos veces el botón lateral.

Para realizar un pago dentro de las apps y en Internet, presiona dos veces el botón lateral para confirmar tu intención de pagar, y autentícate usando Face ID para autorizar el pago. Si tu transacción de Apple Pay no se ha completado 30 segundos después de presionar dos veces el botón lateral, tendrás que volver a presionarlo dos veces para volver a confirmar que quieres realizar el pago.

Diagnóstico de Face ID

Los datos de Face ID no salen de tu dispositivo y nunca se respaldan en iCloud ni en ningún otro lugar. Se transferirá esta información de tu dispositivo únicamente en el caso de que quieras proporcionar datos de diagnóstico de Face ID a AppleCare para fines de soporte. Para activar el diagnóstico de Face ID se requiere una autorización de Apple firmada digitalmente, similar a la que se utiliza en el proceso de personalización de la actualización de software. Después de obtener la autorización, podrás activar el diagnóstico de Face ID e iniciar el proceso de configuración en la app Configuración en tu iPhone X.

Como parte de la configuración del diagnóstico de Face ID, se eliminará tu registro de Face ID existente y se pedirá que vuelvas a registrarte en Face ID. Tu iPhone X empezará a grabar imágenes de Face ID capturadas durante los intentos de autenticación de los próximos 10 días; posteriormente, tu iPhone X dejará de guardar estas imágenes. El diagnóstico de Face ID no envía datos a Apple automáticamente. Puedes revisar y aprobar los datos del diagnóstico de Face ID, incluyendo las imágenes de registro y desbloqueos (tanto fallidos como correctos) que se recopilaron en el modo de diagnóstico, antes de que se envíen a Apple. El diagnóstico de Face ID cargará sólo las imágenes del diagnóstico que apruebes; además, los datos se encriptarán

antes de su carga y se eliminarán de tu iPhone X inmediatamente después de que se haya completado la carga. Las imágenes que rechaces se eliminarán inmediatamente.

Si no concluyes la sesión del diagnóstico de Face ID con la revisión y el envío de las imágenes aprobadas, el diagnóstico de Face ID finalizará automáticamente después de 40 días y se eliminarán de tu iPhone X todas las imágenes. De igual manera, puedes desactivar el diagnóstico de Face ID en cualquier momento. Si lo haces, se eliminarán todas las imágenes locales de inmediato y en estos casos no se compartirán los datos de Face ID con Apple.

Otros usos de Touch ID y Face ID

Las apps de terceros pueden usar las API proporcionadas por el sistema para solicitar al usuario que se autentique utilizando Touch ID, Face ID o un código. Además, las apps compatibles con Touch ID automáticamente admiten Face ID sin necesidad de modificaciones. Cuando se usa Touch ID o Face ID, a la app sólo se le informa si la autenticación se realizó correctamente o no, pero no se le proporciona acceso a Touch ID, Face ID o a los datos asociados con el registro del usuario. Los elementos del llavero también se pueden proteger con Touch ID o Face ID, de modo que el Secure Enclave sólo los pueda desbloquear con una coincidencia correcta o con el código del dispositivo. Los desarrolladores de apps tienen API a su disposición para verificar que el usuario ha establecido un código antes de requerir Touch ID, Face ID o un código para desbloquear los elementos del llavero. Los desarrolladores de apps pueden:

- Requerir que las operaciones API de autenticación no recurran a la contraseña de una app o al código del dispositivo como alternativas. Consultar si un usuario está registrado, lo que permite que se utilice Touch ID o Face ID como un segundo factor en apps en las que la seguridad es muy importante.
- Generar o usar claves ECC dentro del Secure Enclave que pueden estar protegidas por Touch ID o Face ID. Las operaciones que usan estas claves siempre se realizan dentro del Secure Enclave una vez que este autoriza su uso.

También puedes configurar Touch ID o Face ID para aprobar compras de iTunes Store, App Store y iBooks Store, de modo que no tengas que ingresar tu contraseña de Apple ID. Con iOS 11 o posterior, las claves ECC del Secure Enclave protegidas mediante Touch ID y Face ID se usan para autorizar una compra al firmar la solicitud de la tienda.

Encriptación y protección de datos

Borrar todo el contenido y configuración
Esta opción de Configuración borra todas las claves en Effaceable Storage, haciendo que ya no se pueda acceder a ningún dato del usuario en el dispositivo mediante encriptación. Por lo tanto, es una forma ideal de cerciorarse de que toda la información personal se ha eliminado del dispositivo antes de dárselo a otra persona o de devolverlo para su mantenimiento.

Importante: no uses la opción "Borrar todo el contenido y configuración" hasta que hayas realizado un respaldo del dispositivo, ya que los datos eliminados no se podrán recuperar.

La cadena de arranque seguro, la firma de código y la seguridad del proceso de ejecución garantizan que, en un dispositivo, sólo se puedan ejecutar apps y códigos que sean de confianza. iOS dispone de funciones adicionales de encriptación y de protección de datos para proteger los datos del usuario, incluso cuando otras partes de la infraestructura de seguridad estén en peligro (por ejemplo, en un dispositivo con modificaciones no autorizadas). Esto ofrece grandes ventajas tanto a los usuarios como a los administradores de TI, puesto que la información personal y corporativa está protegida en todo momento y se proporcionan métodos para un borrado remoto, inmediato y completo, en caso de robo o pérdida del dispositivo.

Funciones de seguridad de hardware

En dispositivos celulares, la velocidad y la eficiencia energética son factores fundamentales. Las operaciones criptográficas son complejas y pueden provocar problemas de rendimiento o de duración de la batería si no se han tenido en cuenta estas prioridades en las fases de diseño e implementación.

Todos los dispositivos iOS tienen un motor de encriptado AES de 256 bits integrado en la ruta de DMA, entre el almacenamiento flash y la memoria del sistema principal. Esto permite conseguir una encriptación de archivos muy eficiente. En procesadores A9 y posteriores de la serie A, el subsistema de almacenamiento flash se encuentra en un bus aislado que sólo tiene acceso a la memoria que contiene los datos del usuario mediante el motor de encriptado DMA.

El identificador único (UID) del dispositivo y un identificador de grupo (GID) de dispositivos son las claves AES de 256 bits vinculadas (UID) o compiladas (GID) en el procesador de aplicaciones y en el Secure Enclave durante la fabricación. Ningún software ni firmware puede leerlos directamente, sino que sólo pueden ver los resultados de las operaciones de encriptación o desencriptación realizadas por los motores AES dedicados implementados en el silicio con el UID o el GID como clave. Además, sólo el motor AES dedicado al Secure Enclave puede utilizar estos UID y GID del Secure Enclave. El UID y el GID tampoco están disponibles a través de JTAG u otras interfaces de depuración.

En los procesadores T1, S2, S3 y A9 o posteriores de la serie A, cada Secure Enclave genera su propio identificador único (UID). Dado que el UID es único para cada dispositivo, y debido a que se genera íntegramente dentro del Secure Enclave en lugar de en un sistema de manufactura exterior al dispositivo, el UID no está disponible para el acceso o almacenamiento por parte de Apple o cualquiera de sus proveedores. El software que se ejecuta en el Secure Enclave aprovecha el UID para proteger los secretos específicos del dispositivo.

El UID permite vincular los datos a un dispositivo determinado mediante encriptación. Por ejemplo, la jerarquía de claves que protege el sistema de archivos incluye el UID, de modo que si los chips de memoria se trasladan físicamente de un dispositivo a otro, no será posible acceder a los archivos. El UID no está relacionado con ningún otro identificador del dispositivo.

El GID es común en todos los procesadores en una clase de dispositivos (por ejemplo, todos los dispositivos que utilizan el procesador A8 de Apple).

Exceptuando el UID y el GID, todas las claves de encriptado se crean mediante el generador de números aleatorios (RNG) del sistema con un algoritmo basado en CTR_DRBG. La entropía del sistema se genera a raíz de las variaciones en el tiempo de ejecución durante el encendido del dispositivo, y también a causa del tiempo de administración de las interrupciones después del encendido. Las claves generadas en el Secure Enclave utilizan su propio hardware de generación de números aleatorios basado en varios osciladores de anillo que después se procesan con CTR_DRBG.

El borrado seguro de las claves guardadas es tan importante como su generación. Esta tarea es especialmente compleja en almacenamientos flash, por ejemplo, en donde la nivelación de desgaste puede conllevar el borrado de varias copias de datos. Para abordar este problema, los dispositivos iOS incluyen una función dedicada a garantizar el borrado de datos que se conoce como *Effaceable Storage*. Esta función accede a la tecnología de almacenamiento subyacente (por ejemplo, NAND) para acceder y borrar una pequeña cantidad de bloques a un nivel muy bajo.

Protección de datos de archivo

Además de las funciones de encriptación en hardware integradas en los dispositivos iOS, Apple utiliza una tecnología llamada *Protección de datos* para aumentar la protección de los datos almacenados en la memoria flash del dispositivo. La protección de datos no sólo permite que el dispositivo responda ante eventos habituales, como las llamadas de teléfono entrantes, sino que también permite un alto nivel de encriptación para los datos de usuario. En los valores de los datos de apps clave del sistema, como Mensajes, Mail, Calendario, Contactos, Fotos y Salud, se utiliza la protección de datos de forma predeterminada. Además, las apps de terceros instaladas en iOS 7 o posterior también reciben esta protección de forma automática.

La protección de datos se implementa mediante la creación y administración de una jerarquía de claves, y se basa en las tecnologías de encriptación de hardware integradas en cada dispositivo iOS. La protección de datos se controla por archivo, asignando cada archivo a una clase. La accesibilidad se determina dependiendo de si se han desbloqueado o no las claves de la clase. Con la llegada del Sistema de Archivos de Apple (APFS), el sistema de archivos ahora es capaz de subdividir aún más las claves según la extensión (diferentes porciones de un archivo pueden tener diferentes claves).

Visión general de la arquitectura

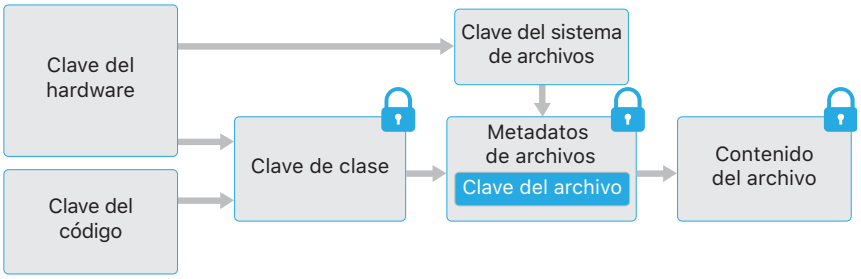
Cada vez que se crea un archivo en la partición de datos, la función de protección de datos crea una nueva clave de 256 bits (la clave "por archivo") y se la proporciona al motor AES de hardware, que utiliza la clave para encriptar el archivo como si se hubiese escrito en la memoria flash con el modo CBC de AES (en dispositivos con un procesador A8 o posteriores, se utiliza AES-XTS). El vector de inicialización (IV) se calcula con el desplazamiento de bloques en el archivo, encriptado con el hash SHA-1 de la clave por archivo.

La clave por archivo (o por extensión) se encapsula con una de las claves de clase, según las situaciones en las que el archivo deba estar accesible. Al igual que en otros casos, esta operación se realiza con la encapsulación de claves AES del NIST, según la publicación RFC 3394. La clave por archivo encapsulada se almacena en los metadatos del archivo.

Los dispositivos que utilizan el sistema de archivos AFS pueden permitir la clonación de archivos (copias sin costo y que utilizan la tecnología de copia al escribir). Si se clona un archivo, cada mitad del archivo clonado obtiene una clave nueva para aceptar escrituras entrantes, de modo que los datos nuevos se escriben en el contenido con una nueva clave. Con el paso del tiempo, el archivo podría estar compuesto de varias extensiones (o fragmentos), y cada una estaría asignada a una clave diferente. Sin embargo, la misma clave de clase protegerá todas las extensiones que comprenden un archivo.

Si se abre un archivo, sus metadatos se desencriptan con la clave del sistema de archivos, lo que revela la clave por archivo encapsulada y una anotación sobre la clase que lo protege. La clave por archivo (o por extensión) se desencapsula con la clave de clase y, después, se proporciona al motor AES de hardware, que desencripta el archivo cuando se lee en la memoria flash. La administración de claves de archivos encapsulados se realiza en el Secure Enclave; la clave de archivo nunca se expone directamente al procesador de aplicaciones. Durante el arranque, el Secure Enclave negocia una clave efímera con el motor AES. Cuando el Secure Enclave desencapsula las claves de un archivo, estas vuelven a encapsularse con la clave efímera y se vuelven a enviar al procesador de aplicaciones.

Los metadatos de todos los archivos del sistema de archivos se encriptan con una clave aleatoria, que se crea la primera vez que se instala iOS o cuando un usuario borra el contenido del dispositivo. En dispositivos compatibles con el sistema de archivos AFS, la clave del UID del Secure Enclave encapsula la clave de los metadatos del sistema de archivos para el almacenamiento a largo plazo. Igual que las claves por archivo o por extensión, la clave de metadatos nunca se expone directamente al procesador de aplicaciones; en su lugar, el Secure Enclave proporciona una versión efímera y única a cada arranque. Cuando está almacenada, la clave del sistema de archivos encriptada se encapsula asimismo en una "clave borrable" almacenada en el Effaceable Storage. Esta clave no proporciona confidencialidad de datos adicional. En cambio, fue diseñada para permitir su borrado rápido por petición (si el usuario usa la opción "Borrar todo el contenido y configuración", o si un usuario o administrador envía un comando de borrado remoto desde una solución MDM, Exchange ActiveSync o iCloud). Al borrar la clave de esta manera, todos los archivos quedan criptográficamente inaccesibles.



El contenido de un archivo puede estar encriptado con una o varias claves por archivo (o por extensión) que se encapsulan con una clave de clase y se almacenan en los metadatos de un archivo, el cual está encriptado con la clave del sistema de archivos. La clave de clase se protege con el UID de hardware y, en el caso de algunas clases, con el código del usuario. Esta jerarquía proporciona flexibilidad y rendimiento. Por ejemplo, para cambiar la clase de un archivo, basta con volver a encapsular su clave por archivo para que luego un cambio de código vuelva a encapsular la clave de clase.

Códigos

Al establecer un código en el dispositivo, el usuario activa automáticamente la protección de datos. iOS acepta códigos alfanuméricos de seis o cuatro dígitos y de longitud arbitraria. Además de desbloquear el dispositivo, un código proporciona entropía para determinadas claves de encriptación. Esto significa que un atacante que haya obtenido un dispositivo no podrá acceder a los datos de clases de protección específicas si no dispone del código,

que está vinculado al UID del dispositivo, por lo que tendría que realizar ataques de fuerza bruta. Para que cada intento sea más lento, se utiliza un recuento de iteraciones elevado. El recuento de iteraciones se calibra de manera que un intento tarde alrededor de 80 milisegundos. Así, se tardaría más de cinco años y medio en intentar todas las combinaciones de un código alfanumérico de seis caracteres que combine minúsculas y números.

Consideraciones sobre la contraseña
Si se ingresa una contraseña larga compuesta únicamente por números, se mostrará un teclado numérico en la pantalla de bloqueo en lugar de un teclado completo. Es posible que sea más fácil ingresar un código numérico largo que un código alfanumérico corto, aunque ambos proporcionen un nivel de seguridad parecido.

Cuanto más seguro sea el código del usuario, más segura será la clave de encriptación. Touch ID y Face ID se pueden usar para mejorar esta ecuación al permitir que el usuario establezca un código mucho más seguro que, de lo contrario, resultaría poco práctico. Con esto se consigue aumentar la entropía real que protege las claves de encriptación utilizadas para la protección de datos, sin que se vea perjudicada la experiencia del usuario al desbloquear un dispositivo iOS muchas veces a lo largo del día.

Demoras entre intentos de ingreso de código

Intentos	Demora aplicada
1–4	ninguna
5	1 minuto
6	5 minutos
7–8	15 minutos
9	1 hora

A fin de desalentar aún más los posibles ataques de fuerza bruta, existen tiempos de demora cada vez mayores después de ingresar un código no válido en la pantalla de bloqueo. Si Configuración > Touch ID y código > "Borrar datos" está activado, el dispositivo realizará un borrado automático después de 10 intentos erróneos consecutivos de ingresar el código. Esta configuración, que se puede definir con un umbral inferior, también está disponible como política de administración a través de MDM y Exchange ActiveSync.

En dispositivos con Secure Enclave, las demoras se aplican mediante el coprocesador Secure Enclave. Si el dispositivo se reinicia durante un tiempo de demora, la demora aún se aplica, con el temporizador empezando de nuevo para el periodo actual.

Clases de protección de datos

Cuando se crea un archivo nuevo en un dispositivo iOS, la app que lo crea le asigna una clase. Cada clase utiliza una política diferente para determinar si se puede acceder a los datos. En las secciones siguientes, se describen las clases y políticas básicas.

Protección completa

(`NSFileProtectionComplete`): la clave de clase está protegida con una clave creada a partir del código de usuario y el UID del dispositivo. Poco después de que el usuario bloquea un dispositivo (10 segundos, si la opción "Solicitar contraseña" está configurada como "Inmediatamente"), se descarta la clave de clase desencriptada y ya no se puede acceder a los datos en esa clase hasta que el usuario vuelva a ingresar el código o desbloquee el dispositivo utilizando Touch ID o Face ID.

Protegido a menos que se abra

(`NSFileProtectionCompleteUnlessOpen`): algunos archivos pueden requerir escritura mientras el dispositivo esta bloqueado. Por ejemplo, al descargar un archivo adjunto de correo en segundo plano. Este proceso se logra utilizando la criptografía de curva elíptica asimétrica (ECDH sobre Curve25519). La clave por archivo usual está protegida por una clave derivada utilizando el acuerdo de clave de Diffie-Hellman de un pase, según se describe en el documento NIST SP 800-56A.

La clave pública efímera del acuerdo se almacena junto la clave por archivo encapsulada. KDF hace referencia a la función de derivación de claves de concatenación (alternativa aprobada 1), tal como se describe en el apartado 5.8.1 de la publicación SP 800-56A del NIST. AlgorithmID se omite; PartyUInfo y PartyVInfo son las claves públicas efímera y estática, respectivamente; mientras que SHA-256 se utiliza como función hash. En cuanto se cierra el archivo, la clave por archivo se borra de la memoria. Para volver a abrir el archivo, se vuelve a crear el secreto compartido mediante la clave privada de la clase Protected Unless Open y la clave pública efímera del archivo; que se usan para desenvolver la clave por archivo que luego se usa para desencriptar el archivo.

Protegido hasta la primera autenticación del usuario

(`NSFileProtectionCompleteUntilFirstUserAuthentication`): esta clase se comporta del mismo modo que Complete Protection, con la diferencia de que la clave de clase desencriptada no se elimina de la memoria al bloquear el dispositivo. La protección de esta clase tiene propiedades similares a la encriptación de volumen completo de escritorio y protege los datos frente a ataques que impliquen un reinicio. Esta es la clase predeterminada para todos los datos de apps de terceros que no tengan una clase de protección de datos asignada por otra vía.

Sin protección

(`NSFileProtectionNone`): esta clave de clase está protegida sólo con el UID y se mantiene en el Effaceable Storage. Dado que todas las claves necesarias para desencriptar los archivos de esta clase se almacenan en el dispositivo, la encriptación sólo agrega la ventaja del borrado remoto rápido. Aunque un archivo no tenga asignada una clase de protección de datos, se almacena en formato encriptado (igual que todos los datos de un dispositivo iOS).

Clave de clase de protección de datos

Clase A	Protección completa	(NSFileProtectionComplete)
Clase B	Protegido a menos que se abra	(NSFileProtectionCompleteUnlessOpen)
Clase C	Protegido hasta la primera autenticación de usuario	(NSFileProtectionCompleteUntilFirstUserAuthentication)
Clase D	Sin protección	(NSFileProtectionNone)

Protección de datos del llavero

Muchas apps necesitan administrar contraseñas y otros datos de pequeño tamaño pero confidenciales, como las claves o los identificadores de inicio de sesión. El llavero de iOS constituye un sistema seguro para almacenar estos elementos.

El llavero se implementa como una base de datos SQLite almacenada en el sistema de archivos. Sólo hay una base de datos; y el daemon securityd determina a qué elementos del llavero puede acceder cada proceso o app. Las API de Acceso a Llaveros generan llamadas al daemon, que envía una consulta a las autorizaciones "keychain-access-groups", "application-identifier" y "application-group" de la app. En lugar de limitar el acceso a un solo proceso, los grupos de acceso permiten que los elementos del llavero se compartan entre apps.

Los elementos del llavero sólo se pueden compartir entre las apps de un mismo desarrollador. Esto se administra solicitando a las apps de terceros que utilicen grupos de acceso con un prefijo asignado a través del programa para desarrolladores de Apple mediante grupos de aplicaciones. El requisito de prefijo y la exclusividad del grupo de aplicaciones se aplican mediante la firma de código, perfiles de datos y el programa para desarrolladores de Apple.

Los datos del llavero se protegen con una estructura de clases similar a la utilizada en la protección de datos de archivo. Estas clases tienen comportamientos equivalentes a las clases de protección de datos de archivo, pero utilizan claves distintas y forman parte de las API con nombres diferentes.

Disponibilidad	Protección de datos de archivo	Protección de datos del llavero
Cuando está desbloqueado	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
Cuando está bloqueado	NSFileProtectionCompleteUnlessOpen	N/A
Después del primer desbloqueo	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Siempre	NSFileProtectionNone	kSecAttrAccessibleAlways
Código activado	N/A	kSecAttrAccessible WhenPasscodeSetThisDeviceOnly

Las apps que utilizan servicios de actualización en segundo plano pueden usar `kSecAttrAccessibleAfterFirstUnlock` para los elementos del llavero a los que sea necesario acceder durante este tipo de actualizaciones.

Componentes de un elemento del llavero

Junto con el grupo de acceso, cada elemento del llavero contiene metadatos de carácter administrativo (como las fechas de creación y de última actualización).

También contiene los hash SHA-1 de los atributos usados para la consulta del elemento (tales como el nombre de cuenta y de servidor) para permitir que se realicen búsquedas sin desencriptar cada elemento. Por último, contiene los datos de encriptación, que incluyen los siguientes:

- Número de versión
- Datos de la lista de control de acceso (ACL)
- Valor que indica en qué clase de protección está el elemento
- Clave por elemento encapsulada con la clave de clase de protección
- Diccionario de atributos que describen el elemento (después de transferirse a SecItemAdd), codificado como un archivo plist binario y encriptado con la clave por elemento

La encriptación es AES 128 en GCM (modo Galois/Counter); el grupo de acceso se incluye en los atributos y se protege con la etiqueta GMAC calculada durante la encriptación.

La clase `kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly` muestra el mismo comportamiento que `kSecAttrAccessibleWhenUnlocked`, sin embargo, sólo está disponible cuando el dispositivo está configurado con un código. Esta clase sólo existe en el depósito de claves del sistema; no se sincroniza con el llavero de iCloud, no se incluye en depósitos de claves de custodia ni se hacen respaldos de ella. Si se elimina o restablece el código, se descartan las claves de clase y los elementos dejan de ser útiles.

Otras clases de llavero tienen un equivalente a "Sólo este dispositivo" que siempre está protegido con el UID cuando se copia de un dispositivo durante un respaldo, de modo que deja de ser útil si se restaura en otro dispositivo.

Apple ha equilibrado la seguridad y la capacidad de uso cuidadosamente mediante la selección de clases de llavero que dependen del tipo de información que se esté protegiendo y de cuándo la necesite iOS. Por ejemplo, un certificado VPN debe estar disponible en todo momento para que el dispositivo esté continuamente conectado, pero se clasifica como "no migratorio" para evitar que se pueda trasladar a otro dispositivo.

En el caso de los elementos de llavero creados por iOS, se aplican las siguientes protecciones de clase:

Elemento	Accesible
Contraseñas de Wi-Fi	Después del primer desbloqueo
Cuentas de Mail	Después del primer desbloqueo
Cuentas de Exchange	Después del primer desbloqueo
Contraseñas de VPN	Después del primer desbloqueo
LDAP, CalDAV y CardDAV	Después del primer desbloqueo
Identificadores de cuentas de redes sociales	Después del primer desbloqueo
Claves de encriptación de anuncios de Handoff	Después del primer desbloqueo
Identificador de iCloud	Después del primer desbloqueo
Contraseña de "Compartir en casa"	Cuando está desbloqueado
Identificador de "Buscar mi iPhone"	Siempre
Buzón de voz	Siempre
Respaldo de iTunes	Cuando está desbloqueado; no migratorio
Contraseñas de Safari	Cuando está desbloqueado
Marcadores de Safari	Cuando está desbloqueado
Certificados VPN	Siempre; no migratorio
Claves de Bluetooth®	Siempre; no migratorio
Identificador del servicio de notificaciones push de Apple	Siempre; no migratorio
Clave privada y certificados de iCloud	Siempre; no migratorio
Claves de iMessage	Siempre; no migratorio
Certificados y claves privadas instalados por un perfil de configuración	Siempre; no migratorio
PIN de la SIM	Siempre; no migratorio

Control de Acceso a Llaveros

Los llaveros pueden utilizar listas de control de acceso (ACL) para establecer políticas de accesibilidad y requisitos de autenticación. Los elementos pueden establecer condiciones que requieran la presencia del usuario al especificar que no se puede acceder a ellos a menos que se lleve a cabo una autenticación con Touch ID, Face ID o que se ingrese el código del dispositivo. De igual manera, se puede limitar el acceso a los elementos al especificar que el registro de Touch ID o Face ID no puede haber cambiado desde que el elemento se agregó. Esta limitación ayuda a prevenir que un atacante agregue su propia huella digital para acceder al elemento de llavero. Las ACL se evalúan en el Secure Enclave y sólo se desbloquean en el kernel si se cumplen las restricciones especificadas.

Acceso a contraseñas guardadas en Safari

Las apps de iOS pueden interactuar con los elementos del llavero guardados en Safari para autorrellenar contraseñas utilizando las dos API siguientes:

- `SecRequestSharedWebCredential`
- `SecAddSharedWebCredential`

Sólo se concederá acceso si tanto el desarrollador de la app como el administrador del sitio web han dado su aprobación; y el usuario, su consentimiento. Los desarrolladores de apps incluyen una autorización en su app para expresar su intención de acceder a las contraseñas guardadas de Safari. En esta autorización se incluye una lista de todos los nombres de dominio válidos de los sitios web asociados. Los sitios web deben colocar un archivo en su servidor que indique los identificadores de app únicos de las apps que han aprobado. Cuando se instala una app con la autorización com.apple.developer.associated-domains, iOS envía una solicitud de TLS a cada sitio web de la lista para solicitar el archivo /apple-app-site-association. Si el archivo incluye el identificador de apps de la app que se está instalando, iOS marcará que el sitio web y la app tienen una relación de confianza. Las llamadas a estas dos API sólo generan una solicitud para el usuario cuando existe una relación de confianza; se requiere la aceptación del usuario para que se lleve a cabo la entrega de contraseñas a la app o para que se actualicen o eliminen.

iOS permite que los usuarios ingresen la información guardada de usuario y contraseña en los campos de credenciales de las apps al tocar una "llave" en la barra de sugerencias QuickType del teclado de iOS. Aprovecha el mismo mecanismo apple-app-site-association para asociar estrechamente las apps y los sitios web. Esta interfaz no revela información de credenciales a la app hasta que el usuario haya aceptado compartir una credencial con la app. Cuando iOS haya establecido una relación de confianza con un sitio web o app, la barra de sugerencias QuickType también recomendará directamente las credenciales para rellenar campos en la app. Esto permite que el usuario elija si se revelan las credenciales guardadas en Safari a las apps que tienen el mismo nivel de seguridad, sin necesidad de que las apps tengan que adoptar una API.

Depósitos de claves

Las claves para las clases de protección tanto de datos de llavero como de archivo se recopilan y administran en depósitos de claves. iOS utiliza los siguientes depósitos de claves: de usuario, de dispositivo, de respaldo, de custodia y de respaldo de iCloud.

El depósito de claves del usuario es el lugar en el que se almacenan las claves de clase encapsuladas que se utilizan durante el funcionamiento normal del dispositivo. Por ejemplo, cuando se ingresa un código, se carga la clave `NSFileProtectionComplete` del depósito de claves del usuario y se desencapsula. Es un archivo plist binario almacenado en la clase "Sin protección", donde los contenidos están encriptados con una clave almacenada en el Effaceable Storage. Con el propósito de proporcionar mayor seguridad a los depósitos de claves, esta clave se borra y se vuelve a generar cada vez que un usuario cambia el código. La extensión del kernel `AppleKeyStore` administra el depósito de claves del usuario y admite consultas relativas al estado de bloqueo del dispositivo. Indica si el dispositivo está desbloqueado sólo si se puede acceder a todas las claves de clase del depósito de claves del usuario. y si se han desencapsulado correctamente.

El depósito de claves del dispositivo se usa para almacenar las claves de clase encapsuladas que se usan para las operaciones que involucran datos específicos del dispositivo. Los dispositivos iOS configurados para uso compartido requieren en ocasiones acceso a credenciales antes de que cualquier usuario pueda iniciar sesión; por lo tanto, se requiere un depósito de claves que no esté protegido por el código del usuario. iOS no es compatible con la separación criptográfica del contenido del sistema de archivos de cada usuario, lo que significa que el sistema usará las claves de clase del depósito de claves del dispositivo para encapsular las claves de cada archivo. El llavero, sin embargo, usa las claves de clase del depósito de claves del usuario para proteger los elementos que se encuentran en el llavero del usuario. En un dispositivo iOS configurado para que lo utilice un único usuario (que es la configuración predeterminada), el depósito de claves del dispositivo y el depósito de claves del usuario son el mismo, y están protegidos por el código del usuario.

El depósito de claves de respaldo se crea cuando iTunes realiza un respaldo encriptado y lo almacena en la computadora donde se efectúa el respaldo del dispositivo. Se crea un depósito de claves nuevo con un conjunto de claves nuevo, y los datos del respaldo se vuelven a encriptar en estas claves nuevas. Como se explicó anteriormente, los elementos no migratorios del llavero permanecen encapsulados con la clave derivada del UID, lo que permite su restauración en el dispositivo desde el cual se respaldaron inicialmente, pero se vuelven inaccesibles desde otros dispositivos.

El depósito de claves está protegido con el conjunto de contraseñas establecido en iTunes, que se ejecuta en 10 millones de iteraciones de PBKDF2. A pesar de la gran cantidad de iteraciones, no existen vínculos a un dispositivo específico y, por lo tanto, los ataques de fuerza bruta realizados en paralelo en muchas computadoras tendrían lugar, teóricamente, en el depósito de claves de respaldo. Esta amenaza se puede mitigar con una contraseña que sea lo suficientemente segura.

Si un usuario opta por no encriptar un respaldo de iTunes, los archivos de respaldo no se encriptan, sea cual sea su clase de protección de datos, pero el llavero sigue estando protegido con una clave derivada del UID. Por este motivo, los elementos del llavero sólo migran a un dispositivo nuevo cuando se establece una contraseña de respaldo.

El depósito de claves de custodia se utiliza para la sincronización con iTunes y MDM. Este depósito de claves permite que iTunes realice un respaldo y la sincronización sin necesidad de que el usuario ingrese un código, y permite que una solución MDM borre de forma remota el código de un usuario. Se almacena en la computadora usada para la sincronización con iTunes, o en la solución MDM que administra el dispositivo.

El depósito de claves de custodia mejora la experiencia del usuario durante la sincronización del dispositivo, que podría requerir el acceso a todas las clases de datos. La primera vez que un dispositivo bloqueado con contraseña se conecta a iTunes, el usuario tiene que ingresar un código. A continuación, el dispositivo crea un depósito de claves de custodia que contiene las mismas claves de clase que se utilizan en el dispositivo, y se protege con una clave recién creada. El depósito de claves de custodia y la clave que lo protege se dividen entre el dispositivo y el host o servidor, y los datos se almacenan en el dispositivo en la clase "Protegido hasta la primera autenticación del usuario". Por eso es necesario ingresar el código del dispositivo antes de que el usuario realice el primer respaldo con iTunes después de un reinicio.

En caso de una actualización de software OTA, el usuario tiene que ingresar su código al inicio del proceso. Este se utiliza para crear de forma segura un identificador de desbloqueo de un solo uso, que desbloquea el depósito de claves del usuario después de la actualización. Este identificador no se puede generar si no se ingresa el código de usuario; todos los identificadores generados anteriormente quedan invalidados si se cambia el código de usuario.

Los identificadores de desbloqueo de un solo uso sirven para instalar con o sin supervisión una actualización de software. Se encriptan con una clave derivada del valor actual de un contador monótono del Secure Enclave, el UUID del depósito de claves y el UID del Secure Enclave.

El incremento del contador de identificadores de desbloqueo de un solo uso del Secure Enclave invalida todos los identificadores existentes. El contador incrementa cuando se utiliza un identificador, después de desbloquear por primera vez un dispositivo reiniciado, cuando se cancela una actualización de software (por parte del usuario o del sistema) o cuando el temporizador de políticas de un identificador ha caducado.

El identificador de desbloqueo de un solo uso para actualizaciones de software con supervisión caduca a los 20 minutos. Este identificador se exporta desde el Secure Enclave y se escribe en Effaceable Storage. Un temporizador de políticas incrementa el contador si el dispositivo no se ha reiniciado en 20 minutos.

Para una actualización de software sin supervisión, establecida cuando el usuario selecciona "Instalar más tarde" al recibir la notificación de la actualización, el procesador de aplicaciones puede mantener la validez del identificador de desbloqueo de un solo uso en el Secure Enclave durante un máximo de 8 horas. Una vez transcurrido ese tiempo, un temporizador de políticas incrementa el contador.

El depósito de claves de respaldo de iCloud es similar al depósito de claves de respaldo. Todas las claves de clase de este depósito son asimétricas (utilizan Curve25519, como la clase de protección de datos "Protegido a menos que se abra"), por lo que es posible realizar respaldos de iCloud en segundo plano. Los datos encriptados se leen en el dispositivo y se envían a iCloud para todas las clases de protección de datos, excepto para la clase "Sin protección". Las claves de clase correspondientes se protegen con claves de iCloud. Las claves de clase del llavero se encapsulan con una clave derivada del UID del mismo modo que los respaldos de iTunes sin encriptar. También se utiliza un depósito de claves asimétrico para el respaldo en el aspecto de recuperación de llaveros del llavero de iCloud.

Certificaciones de seguridad y programas

Nota: para obtener la información más actualizada sobre las instrucciones, validaciones y certificaciones de seguridad de iOS, consulta: https://support.apple.com/es-lamr/HT202739.

Certificaciones ISO 27001 y 27018

Apple tiene las certificaciones ISO 27001 e ISO 27018 del Sistema de Administración de Seguridad de la Información por la infraestructura, desarrollo y operaciones que soportan los productos y servicios: Apple School Manager, iCloud, iMessage, FaceTime, Apple ID administrados y iTunes U, de acuerdo con la Declaración de aplicabilidad 2.1 con fecha del 11 de julio de 2017. El cumplimiento de Apple con la norma ISO fue certificado por la British Standards Institution (BSI). El sitio web de la BSI tiene certificados del cumplimiento de las normas ISO 27001 e ISO 27018. Para ver estos certificados, consulta:

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.

Validación criptográfica (FIPS 140-2)

Los módulos criptográficos de iOS se han validado repetidamente para garantizar su conformidad con las normas del Estándar federal de procesamiento de información de Estados Unidos (FIPS) 140-2 de nivel 1 después de cada lanzamiento desde iOS 6. Como con cada lanzamiento importante, Apple envía los módulos a la CMVP para su revalidación al momento de presentar el sistema operativo iOS. Este programa valida la integridad de las operaciones criptográficas para apps de Apple y de terceros que utilicen correctamente los servicios criptográficos y algoritmos aprobados de iOS.

Certificación de Criterios Comunes (ISO 15408)

Desde el lanzamiento de iOS 9, Apple ha certificado los siguientes elementos de iOS en cada lanzamiento importante de iOS bajo el programa de Certificación de Criterios Comunes (CCC):

- Perfil de protección fundamental para dispositivos móviles
- Perfil de protección para clientes VPN IPSec

- Paquete ampliado para los agentes de administración de dispositivos móviles
- Paquete ampliado para clientes WLAN

El sistema operativo iOS 11 incluye certificaciones para los siguientes elementos:

- Perfil para la protección del software de aplicación
- Paquete ampliado para clientes de correo electrónico
- Paquete ampliado para navegadores web

Apple planea seguir actuando de esta manera en cada lanzamiento importante sucesivo de iOS. Apple ha asumido un papel activo en la Comunidad Técnica Internacional (ITC) para el desarrollo de perfiles de protección colaborativa (CPP) no disponibles actualmente, centrados en la evaluación de tecnología de seguridad móvil clave. Apple continúa evaluando y ampliando certificaciones para versiones nuevas y actualizadas de los perfiles de protección colaborativa disponibles actualmente.

Soluciones Comerciales para Clasificados (CSfC)

En casos donde ha sido necesario, Apple también ha enviado la plataforma iOS y varios servicios para su inclusión en la la lista de componentes de soluciones comerciales para programas clasificados (CSfC). Dado que los servicios y las plataformas de Apple están sujetos a las Certificaciones de Criterios Comunes, también se solicitará su inclusión en la Lista de Componentes de Soluciones Comerciales para Programas Clasificados.

Para consultar la lista con los componentes agregados recientemente, consulta: https://www.nsa.gov/resources/everyone/csfc/components-list/.

Guías de configuración de seguridad

Apple ha colaborado con gobiernos de todo el mundo para desarrollar guías que ofrezcan instrucciones y recomendaciones para mantener un entorno más seguro, también conocido como "endurecimiento de dispositivos para entornos de alto riesgo". Estas guías proporcionan información definida y aprobada sobre cómo configurar y utilizar las funciones integradas de iOS para mejorar la protección.

Seguridad de las apps

Las apps son uno de los elementos más importantes de una arquitectura moderna de seguridad de entornos móviles. Sus ventajas en cuanto a productividad son increíbles, pero si no se administran bien, también pueden repercutir negativamente en la seguridad y estabilidad del sistema, o en los datos de usuario.

Por esta razón, iOS agrega capas de protección para garantizar que las apps estén firmadas y verificadas, además de aisladas para proteger los datos de usuario. Estos elementos proporcionan una plataforma estable y segura para las apps, donde miles de desarrolladores pueden ofrecer sus apps en iOS sin que la integridad del sistema se vea afectada. Además, los usuarios pueden acceder a estas apps en sus dispositivos iOS sin temor a virus, software malicioso o ataques no autorizados.

Firma de código de apps

Una vez que se ha iniciado, el kernel de iOS controla los procesos y apps del usuario que se pueden ejecutar. Para garantizar que todas las apps procedan de una fuente conocida y aprobada, y que no se han manipulado, iOS requiere que todo el código ejecutable se firme con un certificado emitido por Apple. Las apps proporcionadas con el dispositivo, como Mail y Safari, están firmadas por Apple. Las apps de terceros también deben estar validadas y firmadas mediante un certificado emitido por Apple. La firma de código obligatoria extiende el concepto de cadena de confianza del sistema operativo a las apps e impide que apps de terceros carguen código sin firmar o utilicen código que se modifique automáticamente.

Para poder desarrollar e instalar apps en dispositivos iOS, los desarrolladores deben registrarse en Apple y unirse al programa para desarrolladores de Apple. Apple verifica la identidad real de cada desarrollador, ya sea una persona individual o una empresa, antes de emitir su certificado. Este certificado permite a los desarrolladores firmar apps y enviarlas a la tienda App Store para su distribución. Así que todas las apps que están en App Store han sido enviadas por personas u organizaciones identificables, lo cual funciona como elemento disuasorio para la creación de apps maliciosas. Además, Apple las ha revisado para garantizar que funcionan según lo esperado y que no contienen errores ni otros problemas evidentes. Este proceso de revisión, organización y distribución, que se suma a la tecnología ya comentada, da confianza a los clientes en cuanto a la calidad de las apps que compran.

El sistema operativo iOS permite a los desarrolladores incorporar en sus apps infraestructuras que las propias apps o las extensiones incorporadas en ellas pueden utilizar. Para proteger el sistema y otras apps frente a la carga de código de terceros en su espacio de direcciones, el sistema valida la firma de código en todas las bibliotecas dinámicas vinculadas a un proceso al iniciarse. Esta verificación se consigue mediante el identificador de equipo (Team ID), que se extrae de un certificado emitido por Apple. Un identificador de equipo es una cadena de 10 caracteres alfanuméricos, como 1A2B3C4D5F. Un programa puede tener un enlace a cualquier biblioteca de plataformas proporcionada con el sistema o a

cualquier biblioteca que tenga el mismo identificador de equipo en su firma de código que el ejecutable principal. Los ejecutables que se envían con el sistema no cuentan con un identificador de equipo, por lo que sólo pueden contener enlaces a bibliotecas que se envíen con el propio sistema.

Las empresas también pueden crear apps internas para utilizarlas dentro de su organización y distribuirlas a sus empleados. Las empresas y organizaciones pueden solicitar el registro en el Programa Empresas y Desarrolladores de Apple (ADEP) con un número D-U-N-S. Apple aprueba las solicitudes después de verificar la identidad e idoneidad de los solicitantes. Una vez que una organización es miembro de ADEP, puede registrarse para obtener un perfil de datos que permita ejecutar apps internas en los dispositivos autorizados. Los usuarios deben tener instalado el perfil de datos para ejecutar apps internas. De este modo se garantiza que sólo los usuarios que elija la organización puedan cargar las apps en sus dispositivos iOS. Se confía implícitamente en las apps instaladas mediante MDM, dado que la relación entre la organización y el dispositivo ya está establecida. De lo contrario, los usuarios tienen que aprobar el perfil de datos de la app en Configuración. Las organizaciones pueden aplicar restricciones a los usuarios para que no puedan aprobar apps de desarrolladores desconocidos. En el primer lanzamiento de cualquier app empresarial, el dispositivo debe recibir la confirmación positiva de Apple de que se permite ejecutar la app.

A diferencia de otras plataformas móviles, iOS no permite a los usuarios instalar apps procedentes de sitios web que no estén firmadas y puedan ser maliciosas, ni ejecutar código que no sea de confianza. Durante la ejecución, se comprueba la firma de código de todas las páginas de la memoria ejecutable a medida que se cargan para garantizar que una app no se ha modificado desde la última vez que se instaló o actualizó.

Seguridad del proceso de ejecución

Una vez que se ha comprobado que una app procede de una fuente aprobada, iOS pone en marcha medidas de seguridad diseñadas para impedir que ponga en peligro otras apps o el resto del sistema.

Todas las apps de terceros se "aíslan" para impedir que accedan a los archivos almacenados por otras apps o que realicen cambios en el dispositivo. Esto evita que las apps recopilen o modifiquen la información almacenada por otras apps. Cada una tiene un directorio de inicio único para sus archivos, que se asigna de forma aleatoria al instalarla. Si una app de terceros necesita acceder a información ajena, lo hace únicamente mediante los servicios que iOS proporciona de forma explícita.

Los archivos y recursos del sistema también están blindados contra las apps del usuario. iOS se ejecuta, mayormente, como "plataforma móvil" de un usuario sin privilegios, igual que todas las apps de terceros. Toda la partición del sistema operativo se instala como de sólo lectura. Las herramientas que no son necesarias, como los servicios de inicio de sesión remoto, no se incluyen en el software del sistema y las API no permiten que las apps transfieran sus privilegios para modificar otras apps o iOS.

El acceso de apps de terceros a información del usuario y funciones como iCloud, así como su extensibilidad, se controla mediante autorizaciones declaradas. Las autorizaciones son pares de clave-valor que se utilizan para acceder a una app y permiten la autenticación más allá de los factores en tiempo de ejecución, como un ID de usuario UNIX. Las

autorizaciones llevan una firma digital, por lo que no se pueden modificar. Los daemons y las apps del sistema las utilizan mucho para realizar operaciones con privilegios específicos que, de otro modo, requerirían la ejecución del proceso como *root*. Esto reduce considerablemente la posibilidad de que un daemon o una app del sistema en peligro transfiera privilegios.

Además, las apps sólo pueden realizar procesos en segundo plano a través de las API proporcionadas por el sistema. De esta manera, las apps siguen funcionando sin que su rendimiento o la duración de la batería se vean afectados.

La aleatorización del espacio de direcciones (ASLR) protege el sistema frente a los ataques que aprovechan la vulnerabilidad de una memoria dañada. Al abrirse, las apps integradas utilizan la ASLR para garantizar que todas las regiones de la memoria se aleatorizan. La ordenación aleatoria de las direcciones de memoria de código ejecutable, bibliotecas del sistema y estructuras de programación relacionadas reduce la probabilidad de que tengan lugar muchos ataques sofisticados. Por ejemplo, en un ataque "return-to-libc" se intenta engañar a un dispositivo para que ejecute código malicioso mediante la manipulación de las direcciones de memoria de la pila y las bibliotecas del sistema, pero la aleatorización en su colocación dificulta mucho la ejecución del ataque, especialmente en varios dispositivos. Xcode, el entorno de desarrollo de iOS, compila automáticamente programas de terceros que tengan activada la compatibilidad con la ASLR.

iOS aumenta el nivel de protección con la función Execute Never (XN) de ARM, que marca las páginas de memoria como no ejecutables. Sólo las apps en condiciones muy controladas pueden utilizar las páginas de memoria marcadas como grabables y ejecutables: el kernel comprueba la presencia de la autorización de firma de código dinámica exclusiva de Apple. Incluso entonces, sólo se puede realizar una llamada mmap para solicitar una página ejecutable y grabable, a la que se le proporciona una dirección aleatorizada. Safari utiliza esta funcionalidad para su compilador JIT de JavaScript.

Extensiones

iOS permite a las apps proporcionar funcionalidad a otras apps mediante la distribución de *extensiones*. Las extensiones son binarios ejecutables firmados para fines específicos y empaquetados en una app. El sistema detecta las extensiones automáticamente durante la instalación y las pone a disposición de otras apps utilizando un sistema de coincidencias.

Las áreas del sistema que admiten extensiones se conocen como *puntos de extensión*. Cada punto de extensión proporciona API y aplica políticas para el área correspondiente. El sistema determina qué extensiones están disponibles en función de las reglas de coincidencia específicas de cada punto de extensión. El sistema inicia los procesos de extensión automáticamente cuando es necesario y administra su duración. Las autorizaciones se pueden utilizar para restringir la disponibilidad de las extensiones a apps específicas del sistema. Por ejemplo, un widget de la vista Hoy sólo aparece en el centro de notificaciones, y la extensión para compartir sólo está disponible en el panel Compartir. Los puntos de extensión son los widgets "Hoy", "Compartir", "Acciones personalizadas", "Edición de fotos", "Proveedor de documentos" y "Teclado personalizado".

Las extensiones se ejecutan en su propio espacio de direcciones. La comunicación entre la extensión y la app desde la que se ha activado dicha extensión usa comunicación entre procesadores mediada por la estructura del sistema. Las extensiones no tienen acceso a los archivos o espacios de memoria de las otras extensiones. Se han diseñado de forma que estén aisladas entre sí, al igual que de las apps contenedoras y de las apps que las utilizan. Se aíslan igual que cualquier otra app de terceros y tienen un contenedor diferente al de la app que las contiene. Sin embargo, comparten el mismo acceso a los controles de privacidad que la app contenedora. De este modo, si un usuario autoriza el acceso de una app a Contactos, las extensiones incorporadas en la app también gozarán del acceso, pero no así las extensiones activadas por ella.

Los teclados personalizados son un tipo de extensión especial que el usuario activa para todo el sistema. Una vez que se haya activado, la extensión de teclado se utiliza para cualquier campo de texto, excepto para ingresar el código y cualquier vista de texto seguro. Para restringir la transferencia de datos de usuario, los teclados personalizados se ejecutan de forma predeterminada en una zona protegida muy restrictiva que bloquea el acceso a la red, los servicios que realizan operaciones de red en nombre de un proceso y las API que permiten que la extensión sustraiga los datos ingresados. Los desarrolladores de teclados personalizados pueden solicitar que su extensión tenga acceso abierto, lo cual permitiría que el sistema ejecutase la extensión en la zona protegida normal después de obtener el consentimiento del usuario.

En el caso de los dispositivos inscritos en una solución MDM, las extensiones de teclado y documentos obedecen las reglas "Managed Open In". Por ejemplo, la solución MDM puede impedir que un usuario exporte un documento de una app administrada a un proveedor de documentos sin administrar, o que utilice un teclado sin administrar con una app administrada. Además, los desarrolladores de apps pueden impedir el uso de extensiones de teclado de terceros en su app.

Grupos de apps

Las apps y extensiones propiedad de una cuenta de un desarrollador determinado pueden compartir contenido cuando se configuran como parte de un grupos de apps. El desarrollador puede optar por crear los grupos correspondientes en el Portal de desarrolladores de Apple e incluir el conjunto de apps y extensiones que desee. Una vez que se han configurado como parte de un grupo de apps, las apps tienen acceso a lo siguiente:

- Un contenedor en volumen compartido para el almacenamiento, que permanece en el dispositivo mientras al menos una de las apps del grupo esté instalada.
- Preferencias para compartir.
- Elementos del llavero compartidos.

El Portal de desarrolladores de Apple garantiza que los identificadores de grupo de apps sean únicos en todo el ecosistema de apps.

Protección de datos en apps

El kit de desarrollo de software (SDK) de iOS ofrece un conjunto completo de API que facilita a los desarrolladores internos y de terceros la adopción de la protección de datos y contribuye a garantizar el máximo nivel de protección en sus apps. La protección de datos está disponible para las API de archivo y de base de datos, como NSFileManager, CoreData, NSData y SQLite.

La base de datos de la app Mail (archivos adjuntos incluidos), los libros administrados, los marcadores de Safari, las imágenes de apertura de apps y los datos de ubicación también se almacenan encriptados con claves protegidas por el código del usuario en su dispositivo. Las apps Calendario (excepto en los archivos adjuntos), Contactos, Recordatorios, Notas, Mensajes y Fotos implementan la clase "Protegido hasta la primera autenticación del usuario".

Las apps instaladas por el usuario que no activan una clase de protección de datos específica reciben de forma predeterminada la clase "Protegido hasta la primera autenticación de usuario".

Accesorios

El programa de licencias Made for iPhone, iPad y iPod touch (MFi) proporciona a los fabricantes de accesorios aprobados acceso al Protocolo de accesorios para iPod (iAP) y los componentes de hardware necesarios.

Cuando un accesorio MFi se comunica con un dispositivo iOS mediante un conector Lightning o por Bluetooth, el dispositivo pide al accesorio que responda con un certificado proporcionado por Apple, el cual es verificado por el dispositivo con la finalidad de demostrar que cuenta con la autorización de Apple. Entonces, el dispositivo envía un reto, que el accesorio debe contestar con una respuesta firmada. Este proceso está totalmente administrado por un circuito integrado (IC) personalizado que Apple proporciona a los fabricantes de accesorios aprobados y es transparente para el accesorio.

Los accesorios pueden solicitar acceso a distintas funcionalidades y métodos de transporte; por ejemplo, acceso a secuencias de audio digital a través del cable Lightning o información de ubicación proporcionada por Bluetooth. Un circuito integrado de autenticación garantiza que sólo los accesorios aprobados tengan acceso total al dispositivo. Si un accesorio no es compatible con la autenticación, su acceso queda limitado al audio analógico y a un pequeño subconjunto de controles de reproducción de audio en serie (UART).

AirPlay también utiliza el circuito integrado de autenticación para verificar si los receptores cuentan con la aprobación de Apple. Las secuencias de audio de AirPlay y de video de CarPlay utilizan el Protocolo de asociación segura (SAP) MFi, que encripta la comunicación entre el accesorio y el dispositivo con AES-128 en modo CTR. Las claves efímeras se intercambian mediante el intercambio de claves de ECDH (Curve25519) y se firman con la clave RSA de 1024 bits del circuito integrado de autenticación como parte del protocolo de estación a estación (STS).

HomeKit

HomeKit proporciona una infraestructura de automatización doméstica que utiliza la seguridad de iOS y iCloud para proteger y sincronizar los datos privados, sin exponerlos a Apple.

Identidad de HomeKit

La identidad y la seguridad de HomeKit se basan en pares de claves pública y privada Ed25519. En el dispositivo iOS, se genera un par de claves Ed25519 para cada usuario de HomeKit, que pasa a ser su identidad de HomeKit. Dicho par se utiliza para autenticar la comunicación entre dispositivos iOS, y entre accesorios y dispositivos iOS.

Las claves se almacenan en el llavero y sólo se incluyen en los respaldos encriptados del llavero. Se sincronizan entre dispositivos utilizando el llavero de iCloud.

Comunicación con accesorios de HomeKit

Los accesorios de HomeKit generan su propio par de claves Ed25519 para la comunicación con dispositivos iOS. Si el accesorio se restaura con la configuración original de fábrica, se genera un par de claves nuevo.

Para establecer una relación entre un dispositivo iOS y un accesorio de HomeKit, las claves se intercambian utilizando el protocolo de contraseña remota segura (3072 bits) y un código de 8 dígitos proporcionado por el fabricante del accesorio, que el usuario ingresa en el dispositivo iOS, que después se encripta con ChaCha20-Poly1305 AEAD mediante claves derivadas de HKDF-SHA-512. La certificación MFi del accesorio también se verifica durante la configuración.

Cuando el dispositivo iOS y el accesorio de HomeKit se comunican durante el uso, se autentican entre sí mediante las claves intercambiadas en el proceso descrito más arriba. Todas las sesiones se establecen con el protocolo STS y se encriptan con claves derivadas de HKDF-SHA-512 basadas en claves Curve25519 por sesión. Esto aplica tanto a los accesorios basados en IP como a los accesorios Bluetooth LE.

Almacenamiento local de datos

HomeKit almacena datos sobre casas, accesorios, ambientaciones y usuarios en el dispositivo iOS de un usuario. Estos datos almacenados se encriptan con claves derivadas de las claves de identidad de HomeKit del usuario más un valor único aleatorio. Además, los datos de HomeKit se almacenan con la clase de protección de datos "Protegido hasta la primera autenticación de usuario". Los datos de HomeKit sólo se incluyen en respaldos encriptados; así que, por ejemplo, los respaldos de iTunes sin encriptar no contienen datos de HomeKit.

Sincronización de datos entre dispositivos y usuarios

Los datos de HomeKit se pueden sincronizar entre los dispositivos iOS de un usuario mediante iCloud y el llavero de iCloud. Los datos de HomeKit se encriptan durante la sincronización con las claves derivadas de la identidad de HomeKit del usuario y el valor único aleatorio. Estos datos se administran como un objeto binario de gran tamaño (BLOB) opaco durante la sincronización. El BLOB más reciente se almacena en iCloud para permitir la sincronización, pero no se utiliza para ningún otro fin. Además, como está encriptado con claves que sólo están disponibles en los dispositivos iOS del usuario, no es posible acceder a su contenido durante la transmisión y el almacenamiento en iCloud.

Los datos de HomeKit también se sincronizan entre varios usuarios de la misma casa. Este proceso utiliza los mismos métodos de autenticación y encriptación que se usan entre un dispositivo iOS y un accesorio de HomeKit. La autenticación se basa en las claves públicas Ed25519 que se intercambian entre dispositivos al agregar un usuario a una casa. Después de agregar un usuario nuevo a una casa, todas las comunicaciones futuras se autentican y encriptan con el protocolo STS y claves por sesión.

Sólo el usuario que creó el grupo de casa en HomeKit, u otro usuario que tenga permiso de edición, puede agregar usuarios nuevos. El propietario del dispositivo configura los accesorios con la clave pública del nuevo usuario, de modo que el accesorio pueda autenticar y aceptar los comandos de dicho usuario. Cuando un usuario con permisos de edición agrega un usuario nuevo, el proceso se delega a una central de casa para completar la operación.

El proceso de provisión del Apple TV para su uso con HomeKit se realiza de forma automática cuando el usuario inicia sesión en iCloud. La cuenta de iCloud debe tener activada la autenticación de dos factores. El Apple TV y el dispositivo del usuario intercambian temporalmente claves públicas Ed25519 a través de iCloud. Cuando el dispositivo y el Apple TV del propietario están en la misma red local, se usan claves temporales para asegurar la conexión mediante la red local mediante el protocolo de estación a estación (STS) y con claves por sesión. Este proceso utiliza los mismos métodos de autenticación y encriptado que se usan entre un dispositivo iOS y un accesorio de HomeKit. Mediante esta conexión local segura, el dispositivo del propietario transfiere el par de claves pública-privada Ed25519 del usuario al Apple TV. Estas claves se usan para asegurar la comunicación entre el Apple TV y los accesorios HomeKit, así como entre el Apple TV y otros dispositivos iOS que sean parte de la casa de HomeKit.

Si un usuario tiene sólo un dispositivo o no concede acceso a más usuarios al grupo de casa, los datos de HomeKit no se sincronizan en iCloud.

Datos y apps de Casa

El acceso de las apps a los datos de Casa está controlado por la configuración de privacidad del usuario. Para que las apps tengan acceso a estos datos cuando lo solicitan, los usuarios tienen que concedérselo, igual que en el caso de Contactos, Fotos y otras fuentes de datos de iOS. Si el usuario lo autoriza, las apps tienen acceso a los nombres de las habitaciones, los nombres de los accesorios y la ubicación de cada accesorio, así como a otra información que se detalla en la documentación para desarrolladores de HomeKit en: https://developer.apple.com/homekit/.

HomeKit y Siri

Siri se puede utilizar para enviar consultas a los accesorios y controlarlos, y para activar ambientaciones. A Siri se le proporciona de forma anónima una cantidad mínima de información sobre la configuración de la casa para proporcionar nombres de habitaciones, accesorios y ambientaciones necesarias para el reconocimiento de comandos. El audio enviado a Siri podría indicar accesorios o comandos específicos, sin embargo, estos datos de Siri no se asocian con otras funciones de Apple, tales como HomeKit. Para obtener más información, consulta la sección Siri del apartado "Servicios de Internet" de este documento.

Cámaras IP de HomeKit

Las cámaras IP de HomeKit envían transmisiones de video y audio directamente al dispositivo iOS en la red local que accede a la transmisión. Las transmisiones están encriptadas utilizando claves generadas aleatoriamente en el dispositivo iOS y la cámara IP, las cuales se trasladan a la cámara durante la sesión segura de HomeKit. Cuando el dispositivo iOS no se encuentra en la red local, las transmisiones encriptadas se retransmiten mediante una central de casa al dispositivo iOS. La central de casa no desencripta las transmisiones y únicamente funciona como retransmisor entre el dispositivo iOS y la cámara IP. Cuando la app muestra al usuario la vista de video de la cámara IP de HomeKit, HomeKit renderiza los cuadros del video de manera segura mediante un proceso de sistema separado, de modo que la app no puede acceder o almacenar la transmisión de video. Además, las apps no tienen permitido tomar capturas de pantalla de la transmisión.

Acceso remoto a iCloud para accesorios de HomeKit

Los accesorios de HomeKit se pueden conectar directamente con iCloud para permitir su control desde dispositivos iOS cuando no haya disponible una comunicación mediante Bluetooth o Wi-Fi.

El acceso remoto a iCloud está diseñado cuidadosamente de forma que los accesorios puedan controlarse y enviar notificaciones sin revelar a Apple de qué accesorio se trata o qué comandos y notificaciones se están enviando. HomeKit no envía información de la casa a través del acceso remoto a iCloud.

Cuando un usuario envía un comando a través del acceso remoto a iCloud, el accesorio y el dispositivo iOS se autentican mutuamente y los datos se encriptan mediante el mismo procedimiento descrito para conexiones locales. Los contenidos de las comunicaciones se encriptan y Apple no puede verlos. El direccionamiento a través de iCloud se basa en los identificadores de iCloud registrados durante el proceso de configuración.

Los accesorios compatibles con el acceso remoto a iCloud se preparan durante el proceso de configuración del accesorio. El proceso de envío de datos comienza cuando el usuario inicia sesión en iCloud. A continuación, el dispositivo iOS solicita al accesorio que firme un reto mediante el coprocesador de autenticación integrado en todos los accesorios diseñados para HomeKit. El accesorio también genera claves de curva elíptica prime256v1, y la clave pública se envía al dispositivo iOS junto con el reto firmado y el certificado X.509 del coprocesador de autenticación. Estos se utilizan para solicitar un certificado para el accesorio desde el servidor de datos de iCloud. El certificado se almacena en el accesorio, pero no contiene ninguna información de identificación sobre el mismo, aparte del hecho de que tiene permitido acceder al acceso remoto a iCloud de HomeKit. El dispositivo iOS que está realizando el envío de datos también envía un depósito al accesorio, que contiene las URL y otra información necesaria para conectarse al servidor de acceso remoto a iCloud. Esta información no es específica para ningún usuario o accesorio.

Cada accesorio registra una lista de usuarios autorizados con el servidor de acceso remoto a iCloud. La persona que agregó el accesorio a la casa concede a estos usuarios la capacidad de controlar el accesorio. El servidor de iCloud concede un identificador a los usuarios, que puede asignarse a una cuenta de iCloud con el fin de enviar mensajes

de notificación y respuestas de los accesorios. De manera similar, los accesorios disponen de identificadores emitidos por iCloud, pero estos son opacos y no revelan ninguna información sobre el accesorio en sí mismo.

Cuando un accesorio se conecta al servidor de acceso remoto a iCloud de HomeKit, presenta su certificado y una tarjeta. La tarjeta se obtiene de otro servidor de iCloud y no es única para cada accesorio. Cuando un accesorio solicita una tarjeta, incluye su fabricante, modelo y versión de firmware en la solicitud. No se envía ninguna información de identificación del usuario ni de la casa en esta solicitud. La conexión al servidor de tarjetas no se autentica para ayudar a proteger la privacidad.

Los accesorios se conectan al servidor de acceso remoto a iCloud a través de HTTP/2, asegurado mediante TLS 1.2 con AES-128-GCM y SHA-256. El accesorio mantiene abierta la conexión al servidor de acceso remoto a iCloud, de manera que pueda recibir mensajes entrantes y enviar respuestas y notificaciones salientes a los dispositivos iOS.

SiriKit

Siri utiliza el mecanismo de extensión de iOS para comunicarse con apps de terceros. A pesar de que Siri tiene acceso a los contactos de iOS y a la ubicación actual del dispositivo, Siri comprueba los permisos para acceder a los datos protegidos del usuario de la app que contiene la extensión para verificar si la app tiene acceso antes de proporcionarle la información. Siri sólo pasa la parte relevante de la consulta original de usuario a la extensión. Por ejemplo, si la app no tiene acceso a los contactos de iOS, Siri no podrá identificar la relación en una solicitud como "Págale a mi mamá 100 pesos usando <app de pagos>". En este caso, la app de la extensión sólo vería "mamá" a través del fragmento de enunciados en bruto que se le pasan. Sin embargo, si la app sí tiene acceso a los contactos de iOS, recibirá la información de contacto de iOS sobre la mamá del usuario. Si se hizo referencia a un contacto en el cuerpo de un mensaje, por ejemplo, "Dile a mi mamá por la app Mensajes que mi hermano es la onda", Siri no podría identificar "mi hermano" a pesar de las TCC de la app. El contenido presentado por la app podría enviarse al servidor para permitir que Siri entienda el vocabulario que un usuario podría usar en la app.

En casos como "Pídeme un auto para ir a la casa de mi mamá con <nombre de app>", donde la solicitud del usuario requiere información de ubicación de los contactos, Siri proporciona la información de ubicación a la extensión de la app sólo para esa solicitud, independientemente de la ubicación de la app o el acceso a los contactos.

Durante su ejecución, Siri permite a la app compatible con SiriKit que proporcione un conjunto de palabras personalizadas específicas para la instancia de la aplicación. Estas palabras personalizadas están relacionadas con el identificador aleatorio que se explica en la sección Siri en este documento, y tienen la misma vida útil.

HealthKit

HealthKit almacena y agrega datos de apps de salud y condición física con el permiso del usuario. HealthKit también funciona directamente con dispositivos de salud y condición física, tales como monitores de frecuencia cardiaca compatibles con Bluetooth o el coprocesador de movimiento integrado en muchos de los dispositivos iOS.

Datos de salud

HealthKit almacena y agrega los datos de salud del usuario, como su altura, peso, distancia caminada, tensión arterial, etc. Estos datos se almacenan en la clase de protección de datos "Protección completa", de modo que sólo son accesibles cuando el usuario ingresa su código o utiliza Touch ID o Face ID para desbloquear el dispositivo.

HealthKit también agrega datos de administración, como permisos de acceso para apps, nombres de dispositivos conectados a HealthKit e información de programación utilizada para abrir apps cuando hay datos nuevos disponibles. Estos datos se almacenan en la clase de protección de datos "Protegido hasta la primera autenticación de usuario".

Los archivos de registro temporales almacenan los datos de salud que se generan cuando el dispositivo está bloqueado, por ejemplo, cuando el usuario está haciendo ejercicio. Estos datos se almacenan en la clase de protección de datos "Protegido a menos que se abra". Cuando el dispositivo está desbloqueado, los archivos de registro temporales se importan a las bases de datos de salud principales y se eliminan una vez que termina la asociación.

Los datos de salud se pueden almacenar en iCloud. Cuando se configura para usar el almacenamiento de iCloud, los datos de Salud se sincronizan entre dispositivos y se protegen con encriptación que asegura los datos durante la transmisión y el almacenamiento. Los datos de Salud se incluyen sólo en los respaldos de iTunes encriptados. No se incluyen en los respaldos de iTunes ni en los respaldos en iCloud sin encriptar.

Integridad de los datos

En la base de datos, también se almacenan metadatos para hacer un seguimiento de la procedencia de cada registro de datos. Estos metadatos incluyen un identificador de app que identifica la app que almacenó el registro. Además, otros metadatos opcionales pueden contener un respaldo con firma digital. El objetivo es proporcionar integridad de datos para los registros generados por un dispositivo de confianza. La firma digital está en el formato de sintaxis de mensajes criptográficos (CMS) que se especifica en la RFC 5652 del IETF.

Acceso de apps de terceros

El acceso a la API de HealthKit se controla mediante autorizaciones, y las apps deben respetar las restricciones relativas al uso de los datos. Por ejemplo, las apps no pueden utilizar los datos de salud para fines publicitarios. Además las apps tienen que proporcionar a los usuarios una política de privacidad donde se especifique el uso que hacen de los datos de salud.

El acceso de las apps a los datos de salud se controla mediante la configuración de privacidad del usuario. Los usuarios tienen que otorgar acceso a los datos de salud cuando las apps lo solicitan, igual que en el caso de Contactos, Fotos y otras fuentes de datos de iOS. Sin embargo, en el caso de los datos de salud, el acceso que reciben las apps para lectura

de datos es independiente del de escritura y también es independiente por cada tipo de datos de salud. Los usuarios pueden ver y revocar los permisos que se les hayan concedido para el acceso a datos de salud en la pestaña Fuentes de la app Salud.

Si disponen de permiso para escribir datos, las apps también pueden leer los datos que escriban. Si disponen de permiso para leer datos, pueden leer los datos que escriban todas las fuentes. Sin embargo, las apps no pueden saber el acceso que tienen otras apps. Además, las apps no pueden saber con seguridad si disponen de acceso de lectura a los datos de salud. Cuando una app no tiene acceso de lectura, las consultas no devuelven datos, al igual que sucede cuando una base de datos está vacía. Así se evita que las apps infieran el estado de salud del usuario al conocer el tipo de datos que este registra.

Ficha médica

La app Salud permite a los usuarios llenar un formulario con sus datos médicos e información que pueda ser importante durante una emergencia médica. La información se ingresa o actualiza manualmente y no se sincroniza con la información de las bases de datos de salud.

Para ver la información de "Ficha médica", basta con presionar el botón SOS en la pantalla bloqueada. La información se almacena en el dispositivo con la clase de protección de datos "Sin protección", de modo que se pueda acceder a ella sin necesidad de ingresar el código del dispositivo. "Ficha médica" es una función opcional que permite a los usuarios decidir cómo conseguir un equilibrio entre seguridad y privacidad.

ReplayKit

ReplayKit es una infraestructura que permite que los desarrolladores agreguen capacidades de grabación y transmisión en vivo a sus apps. Además, permite que los usuarios agreguen notas a sus grabaciones y transmisiones en vivo usando la cámara frontal del dispositivo y el micrófono.

Grabación de video

Existen varias capas de seguridad integradas en la grabación de un video:

- **Cuadro de diálogo de permisos:** antes de comenzar la grabación, ReplayKit le presenta al usuario una alerta de consentimiento que le solicita acreditar su intención de grabar con la pantalla, el micrófono y la cámara frontal. El aviso se presenta una vez por cada proceso de app, y se volverá a presentar si la app se queda en segundo plano por más de 8 minutos.
- **Captura de audio y pantalla:** la captura de audio y pantalla ocurre fuera del proceso de app en el daemon *replayd* de ReplayKit. Esto asegura que el proceso no tendrá acceso al contenido grabado.
- **Creación y almacenamiento de videos:** el archivo de video se escribe en un directorio al que sólo los subsistemas de ReplayKit pueden acceder, mientras que las apps no pueden. Esto previene que terceras partes usen las grabaciones sin el consentimiento del usuario.
- **Vista previa y uso compartido del usuario final:** el usuario tiene la habilidad de previsualizar y compartir el video con la interfaz de usuario publicada por ReplayKit. La interfaz de usuario se presenta fuera del proceso vía la infraestructura de extensiones de iOS y tiene acceso al archivo de video generado.

Transmisión

- **Captura de audio y pantalla:** el mecanismo de captura de audio y pantalla durante la transmisión es idéntico al de la grabación de video y ocurre en *replayd*.
- **Extensiones de transmisión:** para que los servicios de terceros participen en la transmisión de ReplayKit, deben crear dos nuevas extensiones configuradas con el punto final com.apple.broadcast-services:
  - Una extensión de interfaz de usuario que permita al usuario configurar su transmisión.
  - Una extensión de carga que maneje la carga de datos de audio y video en los servidores de servicios de fondo.
  - La arquitectura garantiza que las apps de alojamiento no tengan privilegios para el contenido de audio y video de la transmisión; sólo ReplayKit y las extensiones de transmisión de terceros tienen acceso.
- **Selector de transmisión:** para seleccionar qué servicio de transmisión utilizar, ReplayKit proporciona un controlador de visualización (similar a UIActivityViewController) que el desarrollador puede presentar en su app. El controlador de visualización se implementa utilizando el SPI de UIRemoteViewController, y se trata de una extensión que se encuentra dentro de la estructura de ReplayKit. No está incluida en el proceso de la app de alojamiento.
- **Extensión de carga:** la extensión de carga que los servicios de transmisión de terceros implementan para manejar contenido de audio y video durante la transmisión puede elegir recibir contenido de dos maneras:
  - Clips pequeños MP4 codificados.
  - Búfers de muestra sin condificar raw.
    - **Manejo de clips MP4:** durante este modo, los pequeños clips MP4 codificados se generan mediante *replayd* y se almacenan en una ubicación privada a la que sólo los subsistemas de ReplayKit pueden acceder. Una vez creado el clip de video, *replayd* pasará la ubicación de este a la extensión de carga de terceros mediante la solicitud SPI NSExtension (basada en XPC). *replayd* también genera un token de área de zona segura de uso único que también se pasa a la extensión de carga, que a su vez otorga a la extensión acceso al clip de video en particular durante la solicitud de extensión.
    - **Manejo del búfer de muestra:** durante este modo, los datos de audio y video se serializan y se pasan a la extensión de carga del tercero en tiempo real a través de una conexión XPC directa. Los datos de video se codifican extrayendo el objeto IOSurface del búfer de muestra del video, codificándolo de forma segura como un objeto XPC, enviándolo a través de XPC a la extensión del tercero y decodificándolo nuevamente y de forma segura en un objeto IOSurface.

Notas seguras

La app Notas incluye la función de notas seguras que permite al usuario proteger el contenido de notas específicas. Las notas seguras se encriptan usando una contraseña proporcionada por el usuario que se solicita para ver las notas en iOS, macOS y en el sitio web de iCloud.

Cuando un usuario protege una nota, se deriva una clave de 16 bytes a partir de la contraseña usando PBKDF2 y SHA256. El contenido de la nota se encripta usando AES-GCM. Los nuevos registros se crean en Core Data y en iCloudKit para almacenar la nota encriptada, la etiqueta y el vector de inicialización; y los registros de la nota original se eliminan (los datos encriptdos no se escriben en su lugar). Los archivos adjuntos se encriptan de la misma forma. Los archivos adjuntos compatibles incluyen imágenes, dibujos, tablas, mapas y sitios web. Las notas que contienen otros tipos de archivos adjuntos no se pueden encriptar, y no se pueden agregar archivos adjuntos que no sean compatibles a las notas que ya están protegidas.

Cuando un usuario ingresa correctamente la contraseña, ya sea para ver o crear una nota protegida, Notas abre una sesión segura. Mientras esta sesión esté abierta, al usuario no se le solicitará que ingrese la contraseña ni que use Touch ID o Face ID para ver o proteger otras notas. Sin embargo, si algunas notas tienen una contraseña distinta, la sesión segura aplica sólo a las notas protegidas con la misma contraseña. La sesión segura se cierra cuando:

- El usuario toca el botón "Bloquear ahora" en Notas.
- Notas permanece en segundo plano durante más de 3 minutos.
- Se bloquea el dispositivo.

Los usuarios que olviden su contraseña aún podrán ver sus notas protegidas o proteger más notas si activan Touch ID o Face ID en sus dispositivos. Además, Notas mostrará una pista proporcionada por el usuario después de tres intentos fallidos de ingresar la contraseña. El usuario debe conocer la contraseña actual para poder cambiarla.

Los usuarios pueden restablecer la contraseña si la han olvidado. Esta función permite que los usuarios creen nuevas notas seguras protegidas usando la nueva contraseña, pero no les permitirá ver las notas protegidas anteriormente. Si el usuario recuerda la contraseña anterior, podrá ver las notas protegidas anteriormente. Para restablecer la contraseña, se requiere la contraseña de la cuenta de iCloud del usuario.

Notas compartidas

Las notas se pueden compartir con otros. Las notas compartidas no están encriptadas de punto a punto. Apple utiliza el tipo de datos encriptados de CloudKit para todo el texto y los archivos adjuntos que el usuario ingrese en una nota. Los componentes siempre se encriptan con una clave que está encriptada en el CKRecord. No se encriptan los metadatos, tales como las fechas de creación y modificación. CloudKit administra el proceso mediante el cual los participantes pueden encriptar o desencriptar los datos de los otros.

Apple Watch

Con la finalidad de proteger los datos del dispositivo, así como las comunicaciones con el iPhone con el que está enlazado y con Internet, el Apple Watch utiliza funciones de seguridad y tecnología diseñadas para iOS. Esto incluye tecnologías como la protección de datos y el control de acceso a llaveros. El código del usuario también está vinculado al UID del dispositivo para crear claves de encriptación.

El enlace entre el Apple Watch y el iPhone se asegura mediante un proceso de fuera de banda (OOB, por sus siglas en inglés) para intercambiar claves públicas, seguido del secreto compartido del enlace de BTLE. El Apple Watch muestra un patrón animado, que captura la cámara del iPhone. Este patrón contiene un secreto codificado que se utiliza para el enlace fuera de banda de BTLE 4.1. En caso necesario, la introducción de la clave de paso de BTLE estándar se utiliza como método de enlace de respaldo.

Una vez establecida la sesión de BTLE, el Apple Watch y el iPhone intercambian sus claves mediante un proceso adaptado desde el IDS, como se describe en la sección sobre iMessage de este documento. Una vez que las claves se han intercambiado, se descarta la clave de la sesión de Bluetooth y todas las comunicaciones entre el Apple Watch y el iPhone se encriptan con ayuda del IDS, con los enlaces encriptados de Bluetooth, Wi-Fi y datos celulares que proporcionan una segunda capa de encriptación. La reversión de la clave se aplica en intervalos de 15 minutos para limitar la ventana de exposición, en caso de que haya algún peligro para el tráfico.

Para respaldar las apps que necesitan datos de transmisión en tiempo real, la encriptación se realiza mediante los métodos descritos en la sección sobre FaceTime del apartado "Servicios de Internet" de este documento, que hacen uso del servicio IDS proporcionado por el iPhone enlazado o una conexión a Internet directa.

El Apple Watch implementa almacenamiento por encriptación de hardware y protección basada en clases para los archivos y los elementos del llavero, como se describe en la sección "Encriptación y protección de datos" de este documento. Además, también se usan depósitos de claves con control de acceso para los elementos del llavero. Las claves que se utilizan para establecer la comunicación entre el reloj y el iPhone también se aseguran mediante la protección basada en clases.

Cuando el Apple Watch no se encuentre dentro del alcance de Bluetooth, se puede usar Wi-Fi o los datos celulares en su lugar. El Apple Watch no se unirá a una red Wi-Fi a menos que las credenciales (que se deben haber sincronizado previamente con el Apple Watch) estén presentes en el iPhone enlazado. Si el Apple Watch está fuera del rango de alcance del iPhone, cualquier credencial de red nueva que esté en el iPhone no estará en el Apple Watch.

El Apple Watch se puede bloquear manualmente manteniendo presionado el botón lateral. Además, se utiliza la heurística del movimiento para intentar bloquear automáticamente el dispositivo poco después de retirarlo de la muñeca. Cuando el Apple Watch está bloqueado, se puede usar Apple Pay únicamente si se ingresa el código del reloj. La detección de la muñeca se desactiva mediante la app Apple Watch del iPhone. Esta configuración también se puede aplicar a través de una solución MDM.

El iPhone enlazado también puede desbloquear el reloj, siempre y cuando el reloj esté en la muñeca. Para ello, se establece una conexión autenticada mediante las claves establecidas durante el proceso de enlace. El iPhone envía la clave, que el reloj utiliza para desbloquear sus claves de protección de datos. El iPhone no conoce el código del reloj, que tampoco se transmite. Esta característica se puede desactivar desde la app Apple Watch del iPhone.

El Apple Watch se puede enlazar sólo con un iPhone a la vez. Cuando se desenlaza, el iPhone comunica instrucciones para que se borren todos los contenidos y los datos del Apple Watch.

Al activar "Buscar mi iPhone" en el iPhone enlazado, también es posible usar el bloqueo de activación en el Apple Watch. El bloqueo de activación dificulta el uso o venta del Apple Watch en caso de pérdida o robo. El bloqueo de activación hace que se requiera el Apple ID y la contraseña del usuario para desenlazar, borrar o reactivar el Apple Watch.

Seguridad de la red

Además de los métodos de protección integrados que Apple utiliza para proteger los datos almacenados en dispositivos iOS, existen muchas medidas de seguridad de la red que las organizaciones pueden poner en marcha para proteger la información durante su transferencia a un dispositivo iOS o desde él.

Los usuarios móviles necesitan acceso a redes corporativas desde cualquier parte del mundo, por lo que es importante garantizar que están autorizados y que sus datos están protegidos durante la transmisión. iOS utiliza —y proporciona acceso de desarrollador— protocolos de red estándar para las comunicaciones autenticadas, autorizadas y encriptadas. Para alcanzar estos objetivos de seguridad, iOS integra tecnologías probadas y los estándares más recientes para conexiones de red de datos celulares y Wi-Fi.

En otras plataformas, se necesita software de firewall para proteger los puertos de comunicación abiertos frente a los intrusos. Dado que iOS reduce la superficie de ataque al limitar los puertos de escucha y al eliminar las utilidades de red innecesarias, como telnet, shell o un servidor web, no se requiere software de firewall adicional en los dispositivos iOS.

TLS

iOS es compatible con los protocolos de seguridad de la capa de transporte (TLS 1.0, TLS 1.1, TLS 1.2) y DTLS. Es compatible tanto con AES-128 como con AES-256, y prefiere conjuntos de encriptación con confidencialidad directa perfecta. Safari, Calendario, Mail y otras apps de Internet utilizan automáticamente este protocolo para activar un canal de comunicación encriptado entre el dispositivo y los servicios de red. Las API de alto nivel (como CFNetwork) facilitan a los desarrolladores la adopción de TLS en sus apps, mientras que las API de bajo nivel (SecureTransport) proporcionan un control muy preciso. CFNetwork no permite SSLv3 y las apps que utilizan WebKit (como Safari) tienen prohibido realizar una conexión SSLv3.

A partir de iOS 11 y macOS High Sierra, no se permiten los certificados de SHA-1 para las conexiones TLS a menos que el usuario confíe en ellos. No se permiten en absoluto los certificados con claves RSA de menos de 2048 bits. El conjunto de encriptación simétrico RC4 está obsoleto en iOS 10 y macOS Sierra. De forma predeterminada, los servidores y clientes TLS con API de SecureTransport no permiten conjuntos de encriptación RC4, y no podrán conectarse cuando RC4 sea el único conjunto de encriptación disponible. Para mayor seguridad, las apps y servicios que requieran RC4 deberían actualizarse para usar conjuntos de encriptación seguros y modernos.

Seguridad de transporte de las apps

La seguridad de transporte de las app proporciona requisitos de conexión de forma predeterminada, de manera que las apps cumplan las buenas prácticas para conexiones seguras al utilizar las API NSURLConnection, CFURL o NSURLSession. De forma predeterminada, la seguridad de transporte de las apps limita la selección de encriptación para que incluya sólo conjuntos que proporcionen confidencialidad directa, específicamente ECDHE_ECDSA_AES y ECDHE_RSA_AES en los modos GCM o CBC. Las apps pueden desactivar el requisito de confidencialidad directa por dominio, en cuyo caso se agrega RSA_AES al conjunto de encriptación disponible.

Los servidores deben ser compatibles con TLS 1.2, Forward Secrecy, y los certificados deben ser válidos y estar firmados mediante SHA-256 o mejor, con una clave RSA de al menos 2048 bits o una clave de curva elíptica de 256 bits como mínimo.

Las conexiones de red que no cumplan estos requisitos darán error, a menos que la app omita la seguridad de transporte de las apps. Los certificados no válidos siempre dan como resultado un fallo grave e imposibilidad de conexión. La seguridad de transporte de las apps se aplica automáticamente a las apps compiladas para iOS 9 o posterior.

VPN

Los servicios de red segura, como las redes privadas virtuales, suelen requerir una configuración mínima para funcionar con dispositivos iOS. Estos funcionan con servidores VPN que admiten los siguientes protocolos y métodos de autenticación:

- IKEv2/IPSec con autenticación por secreto compartido, certificados RSA, certificados ECDSA, EAP-MSCHAPv2 o EAP-TLS.
- SSL-VPN usando la app cliente adecuada de App Store.
- Cisco IPSec con autenticación de usuario mediante contraseña, RSA SecurID o CRYPTOCard, y autenticación de máquina mediante secreto compartido y certificados.
- L2TP/IPSec con autenticación de usuario mediante MS-CHAPV2, RSA SecurID o CRYPTOCard, y autenticación de máquina mediante secreto compartido.

iOS es compatible con lo siguiente:

- "VPN por petición" para las redes que utilizan la autenticación basada en certificados. Las políticas de TI utilizan un perfil de configuración de VPN para especificar los dominios que requieren una conexión VPN.
- "VPN por app" para facilitar las conexiones VPN de forma mucho más granular. MDM puede especificar una conexión para cada app administrada y para dominios específicos en Safari. Esto ayuda a garantizar que los datos seguros siempre entran y salen de la red corporativa, pero no así los datos personales del usuario.

- "VPN siempre activada", que se puede configurar para dispositivos administrados con MDM y que se supervisan con Apple Configurator 2, el Programa de inscripción de dispositivos o Apple School Manager. Así se elimina la necesidad de que los usuarios activen la red VPN para obtener protección al conectarse a redes Wi-Fi y celulares. "VPN siempre activada" proporciona a la organización control absoluto sobre el tráfico del dispositivo al dirigir todo el tráfico IP de vuelta a la organización. El protocolo de túnel por omisión (IKEv2) protege la transmisión de tráfico con encriptación de datos. La organización puede supervisar y filtrar el tráfico de estos dispositivos en ambas direcciones, proteger los datos en la red y restringir el acceso del dispositivo a Internet.

Wi-Fi

iOS es compatible con los protocolos Wi-Fi estándar del sector, incluido WPA2 Enterprise, para así proporcionar acceso autenticado a redes corporativas inalámbricas. WPA2 Enterprise utiliza la encriptación AES de 128 bits para proporcionar a los usuarios la mayor garantía de que sus datos estarán protegidos durante las comunicaciones a través de una conexión de red Wi-Fi. Los dispositivos iOS, compatibles con 802.1X, se pueden integrar en un amplio abanico de entornos de autenticación RADIUS. El iPhone y el iPad son compatibles con los siguientes métodos de autenticación inalámbrica 802.1X: EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0, PEAPv1 y LEAP.

Además de la protección de datos, iOS extiende la protección de nivel WPA2 a los marcos de administración de unidifusión o multidifusión a través del servicio del marco de administración de protección referido en 802.11w. El iPhone 6 y el iPad Air 2 o posterior son compatibles con PMF.

iOS usa una dirección MAC aleatoria al realizar exploraciones Wi-Fi, mientras no esté asociada con una red Wi-Fi. Estas exploraciones podrían realizarse para encontrar y conectarse a una red Wi-Fi preferida, o para ayudar a la función Localización en apps que usan geocercas, tales como los recordatorios basados en la ubicación o para establecer una ubicación en Mapas de Apple. Toma en cuenta que la exploración Wi-Fi que sucede mientras se intenta conectar a la red Wi-Fi preferida no es aleatoria.

iOS también utiliza una dirección MAC aleatoria al realizar exploraciones de preferencia de descarga de red mejorada (ePNO) cuando un dispositivo no está asociado a una red Wi-Fi o su procesador está en reposo. Las exploraciones ePNO se ejecutan cuando un dispositivo utiliza Localización para apps con geocercas, como los recordatorios basados en la ubicación que determinan si el dispositivo se encuentra cerca de una ubicación específica.

Ahora la dirección MAC de un dispositivo cambia cuando no está conectado a una red Wi-Fi, por lo que no se puede utilizar para realizar un seguimiento continuo de un dispositivo con observadores pasivos del tráfico de la red Wi-Fi, incluso cuando el dispositivo está conectado a una red celular. Apple ha informado a los fabricantes de Wi-Fi que las exploraciones Wi-Fi de iOS utilizan una dirección MAC aleatoria, y que ni Apple ni los fabricantes pueden predecir estas direcciones MAC aleatorias. El iPhone 4s o modelos anteriores no cuentan con soporte para las direcciones MAC aleatorias para Wi-Fi.

En el iPhone 6S o modelos posteriores, la propiedad oculta de una red Wi-Fi familiar es conocida y se actualiza automáticamente. Si el SSID de una red Wi-Fi se transmite, el dispositivo iOS no envía una prueba con el SSID incluido en la solicitud. Esto evita que el dispositivo transmita el nombre de redes que no están ocultas.

Para proteger el dispositivo de vulnerabilidades en el firmware del procesador de la red, las interfaces de la red —incluyendo redes Wi-Fi y banda base— tienen acceso limitado a la memoria del procesador de apps. Cuando se usa USB o SDIO para interactuar con el procesador de la red, este no puede iniciar transacciones de acceso directo a memoria (DMA) hacia el procesador de apps. Cuando se usa PCIe, cada procesador de red funciona como su propio bus PCIe aislado. Un IOMMU en cada bus PCIe limita el acceso directo a memoria (DMA) del procesador de red a las páginas de la memoria que contienen sus paquetes de red o estructuras de control.

Bluetooth

La conectividad Bluetooth en iOS está diseñada de modo que su funcionalidad resulte útil y que el acceso a datos privados no aumente innecesariamente. Los dispositivos iOS admiten conexiones Encryption Mode 3, Security Mode 4 y Service Level 1. iOS es compatible con los siguientes perfiles de Bluetooth:

- Perfil de manos libres (HFP 1.5)
- Perfil de acceso a la agenda telefónica (PBAP)
- Perfil de acceso a mensajes (MAP)
- Perfil de distribución de audio avanzado (A2DP)
- Perfil de control remoto de audio/video (AVRCP)
- Perfil de red de área personal (PAN)
- Perfil de dispositivo de interfaz humana (HID)
- La compatibilidad con estos perfiles varía en función del dispositivo.

Para obtener más información, consulta: https://support.apple.com/es-lamr/ht3647.

Inicio de sesión único (SSO)

iOS admite la autenticación en redes empresariales mediante el inicio de sesión único (SSO). El SSO funciona con redes basadas en Kerberos para autenticar a usuarios en los servicios a los que tienen permitido el acceso. El SSO se puede utilizar para diferentes operaciones de red, desde la navegación segura en Safari hasta el uso de apps de terceros. También admite la autenticación basada en certificados (PKINIT).

En el SSO de iOS, se utilizan identificadores SPNEGO y el protocolo HTTP Negotiate para trabajar con puertas de enlace de autenticación basada en Kerberos y sistemas de autenticación integrada de Windows que admitan vales de Kerberos. La compatibilidad con el SSO se basa en el proyecto de código abierto Heimdal.

Se admiten los siguientes tipos de encriptación:

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari admite el SSO, y también se pueden configurar las apps de terceros que utilizan API de conexión a redes de iOS estándar para que lo hagan. Para configurar el SSO, iOS admite una carga de perfil de configuración que permite a las soluciones MDM obtener la configuración necesaria. Aquí se incluye el nombre del principal usuario (es decir, la cuenta de usuario de Active Directory) y la configuración del reino Kerberos, así como la configuración de las apps y direcciones URL web de Safari a las que se debe permitir el uso del SSO.

Seguridad de AirDrop

Los dispositivos iOS compatibles con AirDrop utilizan Bluetooth de baja energía (BLE o Bluetooth LE) y la tecnología Wi-Fi P2P creada por Apple para enviar archivos e información a dispositivos cercanos, incluidos las computadoras Mac compatibles con AirDrop que ejecuten OS X 10.11 o posterior. El radio de alcance Wi-Fi sirve para la comunicación directa entre dispositivos sin utilizar ningún tipo de conexión a Internet ni punto de acceso Wi-Fi.

Cuando un usuario activa AirDrop, se almacena una identidad RSA de 2048 bits en el dispositivo. Además, se crea un hash de identidad de AirDrop basado en las direcciones de correo electrónico y los números de teléfono asociados al Apple ID del usuario.

Cuando un usuario elige AirDrop como método para compartir un elemento, el dispositivo emite una señal de AirDrop a través de Bluetooth LE. Los dispositivos que estén activos, se encuentren cerca y tengan AirDrop activado detectarán la señal y responderán con una versión abreviada del hash de identidad de su propietario.

La configuración predeterminada de AirDrop para compartir es "Sólo contactos". Los usuarios también pueden optar por utilizar AirDrop con la opción de compartir con todos o desactivar la función por completo. En el modo "Sólo contactos", los hashes de identidad recibidos se comparan con los hashes de las personas incluidas en la app Contactos del iniciador. Si se encuentra una coincidencia, el dispositivo emisor crea una red Wi-Fi P2P y anuncia que hay una conexión AirDrop a través de Bonjour. Los dispositivos receptores utilizan esta conexión para enviar al iniciador sus hashes de identidad completos. Si el hash completo sigue coincidiendo con Contactos, el nombre y la foto del destinatario (si se encuentra en Contactos) se muestran en la hoja de compartir de AirDrop.

Cuando se utiliza AirDrop, el usuario emisor selecciona a los usuarios con los que desea compartir. El dispositivo emisor inicia una conexión encriptada (TLS) con el dispositivo receptor, que intercambia sus certificados de identidad de iCloud. La identidad de los certificados se coteja con la información disponible en la app Contactos de cada usuario. A continuación, se solicita al usuario receptor que acepte la transferencia entrante de la persona o el dispositivo identificados. Si se eligieron varios destinatarios, este proceso se repite para cada destino.

En el modo "Todos", se utiliza el mismo proceso. Sin embargo, cuando no se encuentra una coincidencia en Contactos, los dispositivos receptores se muestran en la hoja de envío de AirDrop con una silueta con el nombre del dispositivo, tal como se indica en Configuración > General > Información > Nombre.

Las organizaciones pueden restringir el uso de AirDrop para los dispositivos o apps administradas mediante una solución MDM.

Compartir contraseña de Wi-Fi

Los dispositivos iOS que permiten compartir contraseñas de Wi-Fi usan un mecanismo similar a AirDrop para enviar una contraseña de Wi-Fi de un dispositivo a otro.

Cuando un usuario selecciona una red Wi-Fi (solicitante) y se le pide que ingrese la contraseña de la red Wi-Fi, el dispositivo Apple inicia una solicitud mediante Bluetooth LE para indicar que requiere la contraseña de la red Wi-Fi. Otros dispositivos de Apple que estén activados, cerca y que tengan la contraseña de la red Wi-Fi seleccionada, se conectan al dispositivo solicitante mediante Bluetooth LE.

El dispositivo que tiene la contraseña de Wi-Fi (otorgante) requiere la información de contacto del solicitante, y el solicitante debe verificar su identidad utilizando un mecanismo similar al de AirDrop. Después de verificar la identidad, el otorgante envía al solicitante la clave PSK de 64 caracteres, la cual también sirve para unirse a la red.

Las organizaciones pueden restringir la opción de compartir contraseñas de Wi-Fi en dispositivos o apps administradas mediante una solución MDM.

Apple Pay

Con Apple Pay, los usuarios pueden utilizar el Apple Watch y los dispositivos iOS compatibles para pagar de forma sencilla, segura y privada en tiendas, apps y en la web mediante Safari. Es un sistema fácil para los usuarios que incluye seguridad integrada tanto en el hardware como en el software.

Además Apple Pay está diseñado para proteger la información personal del usuario. Apple Pay no recopila información de las transacciones que se pueda vincular al usuario. Las transacciones de pago quedan entre el usuario, el beneficiario y la entidad emisora de la tarjeta.

Componentes de Apple Pay

Secure Element: el Secure Element es un chip estándar certificado en el que se ejecuta la plataforma Java Card, que cumple con los requisitos del sector financiero en cuanto a pagos electrónicos.

Controlador NFC: el controlador de comunicación de corto alcance (NFC) administra los protocolos NFC y dirige la comunicación entre el procesador de aplicaciones y el Secure Element, y entre el Secure Element y el terminal del punto de venta.

Wallet: este componente se utiliza para agregar y administrar tarjetas de crédito, débito, recompensas o cliente para hacer pagos con Apple Pay. Los usuarios pueden ver sus tarjetas e información adicional sobre la entidad emisora de la tarjeta, la política de privacidad de la entidad emisora de la tarjeta, las transacciones recientes y otros datos en Wallet. También pueden agregar tarjetas a Apple Pay en el Asistente de Configuración y en Configuración.

Secure Enclave: en el iPhone, iPad y Apple Watch, el Secure Enclave administra el proceso de autenticación y permite realizar transacciones de pago.

En el caso del Apple Watch, el dispositivo debe estar desbloqueado y el usuario debe presionar dos veces el botón lateral. Al detectar que se presiona el botón dos veces, la acción se transfiere directamente al Secure Element, o Secure Enclave si está disponible, directamente sin pasar por el procesador de aplicaciones.

Servidores de Apple Pay: los servidores de Apple Pay administran la configuración y distribución de tarjetas de crédito y débito en Wallet y los números de cuenta del dispositivo almacenados en el Secure Element. Se comunican tanto con el dispositivo como con los servidores de la red de pagos. Los servidores de Apple Pay también son los responsables de volver a encriptar las credenciales de pago para los pagos realizados desde las apps.

Cómo Apple Pay usa el componente Secure Element

Secure Element aloja un applet diseñado específicamente para administrar Apple Pay. También incluye applets de pago certificados por las redes de pago. Los datos de las tarjetas de crédito, débito o prepago se envían a estos applets de pago desde la red de pago o la entidad emisora de la tarjeta, encriptados con claves que sólo conocen la red de pago y el dominio de seguridad de los applets de pago. Estos datos se almacenan en los applets de pago y se protegen con las funciones de seguridad del Secure Element. Durante una transacción, la terminal se comunica directamente con el Secure Element a través del controlador NFC mediante un bus de hardware dedicado.

Cómo Apple Pay usa el controlador NFC

Como puerta de enlace al Secure Element, el controlador NFC garantiza que todas las transacciones de pago sin contacto se realicen a través de una terminal de punto de venta que esté cerca del dispositivo. El controlador NFC sólo marca como transacciones sin contacto aquellas solicitudes de pago procedentes de una terminal del área.

Una vez que el titular de la tarjeta autoriza el pago mediante Touch ID o su código, o bien al presionar dos veces botón lateral de un Apple Watch desbloqueado, el controlador dirige las respuestas sin contacto preparadas por los applets de pago del Secure Element al campo de NFC de forma exclusiva. En consecuencia, los datos de autorización de pagos para las transacciones sin contacto se incluyen en el campo local de NFC y nunca se exponen al procesador de aplicaciones. En comparación, los datos de autorización de pagos realizados en las apps y en la web se dirigen al procesador de apps, pero siempre después de que el Secure Element los encripte en el servidor de Apple Pay.

Datos de tarjetas de crédito, débito y prepago

Cuando un usuario agrega una tarjeta de crédito, débito o prepago (incluidas las tarjetas cliente) a Apple Pay, Apple envía la información de la tarjeta, junto con otra información sobre la cuenta y el dispositivo del usuario, a la entidad emisora o al proveedor de servicios autorizado de la entidad emisora de la tarjeta de forma segura. La entidad emisora de la tarjeta utiliza esta información para decidir si aprueba agregar la tarjeta a Apple Pay.

Apple Pay utiliza tres llamadas del servidor para la comunicación con la entidad emisora de la tarjeta o la red como parte del proceso de envío de datos de tarjetas: "Campos obligatorios", "Comprobar tarjeta" y "Enlazar y enviar datos". La entidad emisora de la tarjeta o la red utilizan estas llamadas para verificar, aprobar y agregar tarjetas a Apple Pay. Estas sesiones cliente-servidor se encriptan con TLS 1.2.

En el dispositivo y los servidores de Apple, no se almacenan los números de tarjeta completos, sino que se crea un número de cuenta de dispositivo encriptado que después se almacena en el Secure Element. Este número único se encripta de forma que Apple no pueda acceder a él. El número de cuenta de dispositivo es único y diferente de los números de tarjeta de crédito o débito habituales; la entidad emisora de la tarjeta puede impedir su uso en tarjetas de banda magnética, por teléfono o en sitios web.

En el Secure Element, el número de cuenta de dispositivo está aislado de iOS y watchOS, y nunca se almacena en los servidores de Apple ni se incluye en los respaldos de iCloud.

Las tarjetas que se utilizan con el Apple Watch se transmiten a Apple Pay mediante la app Apple Watch del iPhone. Para transmitir una tarjeta al Apple Watch es necesario que el reloj esté dentro del radio de alcance de Bluetooth. Las tarjetas están registradas específicamente para su uso con el Apple Watch y disponen de sus propios números de cuenta de dispositivo almacenados en el Secure Element del Apple Watch. Existen tres maneras de enviar una tarjeta de crédito, débito o prepago a Apple Pay:

- Agregar una tarjeta manualmente a Apple Pay.
- Agregar tarjetas de crédito o débito registradas en una cuenta de iTunes Store a Apple Pay.
- Agregar tarjetas desde la app de la entidad emisora de la tarjeta.

Agregar una tarjeta de crédito o débito manualmente a Apple Pay

Para agregar una tarjeta manualmente, incluidas las tarjetas cliente, se utilizan el nombre, el número de la tarjeta de crédito, la fecha de caducidad y el código CVV con el fin de facilitar el proceso de envío de datos. Desde Configuración, la app Wallet o la app Apple Watch, los usuarios pueden ingresar dicha información mediante el teclado o utilizando la cámara del dispositivo. Cuando la cámara captura la información de la tarjeta, Apple intenta rellenar los campos de nombre, número de tarjeta y fecha de caducidad. La foto no se guarda nunca en el dispositivo ni se almacena en la fototeca. Una vez que todos los campos estén completos, en el proceso "Comprobar tarjeta" se verifican todos los campos excepto el código CVV. Esta información se encripta y envía al servidor de Apple Pay.

Si se devuelve un identificador de condiciones de uso con el proceso "Comprobar tarjeta", Apple descarga las condiciones de la entidad emisora de la tarjeta y se las muestra al usuario. Si el usuario las acepta, Apple envía el identificador de las condiciones aceptadas y el código CVV al proceso "Enlazar y enviar datos". De forma adicional y como parte del proceso "Enlazar y enviar datos", Apple comparte información desde el dispositivo con la entidad emisora de la tarjeta o la red, como información acerca de tu actividad en las tiendas iTunes Store y App Store (por ejemplo, si dispones de un amplio historial de transacciones dentro de iTunes), información acerca de tu dispositivo (por ejemplo, el número de teléfono, el nombre y el modelo del dispositivo, así como de cualquier dispositivo iOS con el que está enlazado y que es necesario para configurar Apple Pay) y tu ubicación aproximada al momento de agregar tu tarjeta (si tienes activada la función Localización). La entidad emisora de la tarjeta utiliza esta información para decidir si aprueba agregar la tarjeta a Apple Pay.

El proceso de enlace y envío de datos tiene dos consecuencias:

- El dispositivo empieza a descargar el archivo de Wallet correspondiente a la tarjeta de crédito o débito.
- El dispositivo empieza a vincular la tarjeta al Secure Element.

El archivo de la tarjeta contiene varias direcciones URL para descargar imágenes y metadatos de la tarjeta (p. ej., la información de contacto), la app de la entidad emisora de la tarjeta correspondiente y otras funciones compatibles. También contiene su estado, que incluye información como,

por ejemplo, si se ha completado la personalización del Secure Element, si la entidad emisora de la tarjeta ha suspendido su uso, o bien si es necesario realizar otra verificación antes de poder pagar con la tarjeta mediante Apple Pay.

Agregar tarjetas de crédito o débito registradas en una cuenta de iTunes Store a Apple Pay

En el caso de una tarjeta de crédito o débito que ya esté registrada en iTunes, el usuario tendrá que volver a ingresar la contraseña de su Apple ID. El número de la tarjeta se obtiene desde iTunes y se inicia el proceso "Comprobar tarjeta". Si la tarjeta es compatible con Apple Pay, el dispositivo descargará y mostrará las condiciones de uso y luego enviará la información sobre el ID y el código de seguridad de la tarjeta para pasar al proceso "Enlazar y enviar datos". Puede que se realice una verificación adicional en el caso de las tarjetas de las cuentas de iTunes registradas.

Agregar tarjetas de crédito o débito desde la app de la entidad emisora de la tarjeta

Cuando la app está registrada para su uso con Apple Pay, se establecen claves para el servidor del beneficiario y la app. Estas claves se utilizan para encriptar la información de la tarjeta que se envía al beneficiario, lo que impide que el dispositivo iOS pueda leer dicha información. El flujo de envío de datos es similar al que se utiliza para tarjetas agregadas de forma manual, descrito anteriormente, exceptuando que se utilizan contraseñas de un solo uso en lugar del código CVV.

Verificación adicional

La entidad emisora de la tarjeta puede decidir si una tarjeta de crédito o débito requiere una verificación adicional. En función de la oferta de la entidad emisora de la tarjeta, es posible que el usuario pueda elegir entre diferentes opciones para realizar la verificación adicional. Tales opciones pueden ser, entre otras, un mensaje de texto, un mensaje de correo electrónico, una llamada del servicio de atención al cliente o un método para finalizar la verificación en la app aprobada de un tercero. Para los mensajes de texto o de correo electrónico, el usuario selecciona la información de contacto entre los datos que la entidad emisora de la tarjeta tiene registrados. A continuación, se envía un código que el usuario necesitará ingresar en Wallet, Configuración o la app Apple Watch. En el caso de servicio al cliente y verificación mediante una app, el emisor realiza su propio proceso de comunicación.

Autorización de pagos

En los dispositivos que tienen Secure Enclave, el Secure Element permitirá que se realice un pago sólo después de recibir la autorización de Secure Enclave. En iPhone o iPad, esto implica confirmar que el usuario se ha autenticado con Touch ID, Face ID o el código del dispositivo. Si está disponible, Touch ID o Face ID es el método predeterminado, pero siempre se puede usar el código. Después de tres intentos erróneos de reconocimiento de la huella digital, o dos intentos fallidos de reconocimiento facial, se ofrece la posibilidad de ingresar el código. Después de cinco intentos erróneos, es obligatorio ingresar el código. Además, el código también es necesario si las funciones Touch ID o Face ID no están configuradas o activadas para Apple Pay. En Apple Watch, el dispositivo debe haberse desbloqueado con el código y se debe presionar dos veces el botón lateral para realizar un pago.

La comunicación entre el Secure Enclave y el Secure Element se realiza mediante una interfaz serial, con el Secure Element conectado al controlador NFC que, a su vez, se conecta al procesador de aplicaciones. Aunque no estén directamente conectados, el Secure Enclave y el Secure Element se pueden comunicar de forma segura gracias a una clave de enlace suministrada durante el proceso de fabricación. La encriptación y la autenticación de la comunicación se basan en el estándar AES, con identificadores temporales criptográficos que usan ambas partes para protegerse de los ataques de reproducción. La clave de enlace se genera dentro del Secure Enclave a partir de la clave UID y el identificador único del Secure Element. Después, se transfiere del Secure Enclave a un módulo de seguridad de hardware (HSM) en la fábrica, que dispone del material necesario para ingresar la clave de enlace en el Secure Element.

Cuando el usuario autoriza una transacción, el Secure Enclave envía datos firmados acerca del tipo de autenticación e información detallada sobre el tipo de transacción (sin contacto o desde apps) al Secure Element, que está vinculado a un valor de autorización aleatorio (AR). Este valor se genera en el Secure Enclave cuando un usuario facilita por primera vez una tarjeta de crédito, y no cambia mientras Apple Pay está activado. La encriptación del Secure Enclave y el mecanismo antirretroceso protegen este valor, que se envía de forma segura al Secure Element mediante la clave de enlace. Al recibir un valor AR nuevo, el Secure Element marca como eliminada cualquier tarjeta agregada previamente.

Las tarjetas de crédito, débito o prepago que se hayan agregado al Secure Element solamente se pueden usar si este muestra una autorización con la misma clave de enlace y el mismo valor AR que cuando se agregó la tarjeta. Esto permite que iOS dé instrucciones al Secure Enclave para que inhabilite las tarjetas marcando su copia del valor AR como no válida en las siguientes circunstancias:

- Si se desactiva el código.
- Si el usuario cierra su sesión en iCloud.
- Si el usuario selecciona "Borrar contenido y configuración".
- Si el dispositivo se restaura desde el modo de recuperación.

Con el Apple Watch, las tarjetas se marcan como no válidas en los siguientes casos:

- Se desactiva el código de acceso en el reloj.
- Se desenlaza el reloj del iPhone.
- Se desactiva la detección de la muñeca.

Mediante el uso de la clave de enlace y su copia del valor AR actual, el Secure Element verifica la autorización que recibió del Secure Enclave antes de activar el applet de pago en el caso de un pago sin contacto. Este proceso también se aplica cuando se obtienen los datos de pago encriptados de un applet de pago para realizar transacciones desde apps.

Código de seguridad dinámico específico para cada transacción

Las transacciones de pago que se originan en los applets de pago incluyen un código de seguridad dinámico específico para cada transacción junto con un número de cuenta del dispositivo. Este código de un solo uso se calcula con la ayuda de un contador, que se incrementa con cada nueva transacción, y una clave, que se proporciona en el applet de pago durante su personalización y que la red de pago o la entidad emisora de la tarjeta conocen. Dependiendo del sistema de pago, puede que también se usen otros datos para calcular estos códigos, entre los que se incluyen:

- Un número aleatorio que genera el applet de pago.
- Otro número aleatorio que genera la terminal (en caso de tratarse de una transacción NFC)

  o bien

- otro número aleatorio que genera el servidor (en caso de tratarse de transacciones realizadas desde apps).

Estos códigos de seguridad se proporcionan tanto a la red de pago como a la entidad emisora de la tarjeta y les sirven de herramienta para la verificación de cada transacción. La longitud de esos códigos de seguridad puede variar en función del tipo de transacción que se realice.

Pagos sin contacto con Apple Pay

Si el iPhone está encendido y detecta un campo NFC, mostrará al usuario la tarjeta de crédito, débito o prepago correspondiente, o bien la tarjeta predeterminada (que se administra desde Configuración). El usuario también puede ir a la app Wallet y seleccionar una tarjeta de crédito o débito; o cuando el dispositivo esté bloqueado, puede presionar dos veces el botón de inicio.

A continuación, el usuario deberá autenticarse mediante Touch ID, Face ID, o su código antes de que se transmita la información relativa al pago. Si el Apple Watch está desbloqueado, presionar dos veces el botón lateral hace que se active la tarjeta predeterminada para realizar el pago. No se envía ninguna información de pago sin la autenticación del usuario. Al procesar el pago una vez que el usuario se ha autenticado, se utiliza el número de cuenta del dispositivo y un código de seguridad dinámico específico para cada transacción. Ni Apple ni ningún dispositivo del usuario enviarán los números completos de la tarjeta de crédito o débito actual a los beneficiarios. Puede que Apple reciba información anónima relacionada con la transacción como, por ejemplo, la ubicación y la hora aproximada en la que se realizó. Esta información sirve de ayuda para mejorar Apple Pay, así como otros productos y servicios de Apple.

Pagos con Apple Pay desde apps

También se puede usar Apple Pay para realizar pagos dentro de las apps de iOS y del Apple Watch (a partir de watchOS 3). Cuando los usuarios pagan dentro de las apps mediante Apple Pay, Apple recibe información encriptada de la transacción y vuelve a encriptarla con una clave específica del desarrollador antes de enviarla a dicho desarrollador o comercio. Apple Pay guarda información sobre la transacción de forma anónima como, por ejemplo, el importe aproximado de la compra. Esta información no permite identificar al usuario y nunca incluye lo que se compró.

Cuando una app inicia una transacción de pago de Apple Pay, los servidores de Apple Pay reciben la transacción encriptada desde el dispositivo antes de que el beneficiario la reciba. A continuación, los servidores de Apple Pay vuelven a encriptarla con la clave específica del beneficiario antes de transmitirle la transacción.

Cuando una app solicita un pago, llama a una API para determinar si el dispositivo es compatible con Apple Pay y si la tarjeta de crédito o débito del usuario puede utilizarse para realizar pagos en una red de pago que acepte el beneficiario. La app solicita todos los datos que necesita para procesar y completar la transacción tal como las direcciones de envío y facturación, o la información de contacto. A continuación, la app pide a iOS que presente la hoja de Apple Pay, que solicita información para la app, así como otra información necesaria, como la tarjeta que se va a utilizar.

Es entonces cuando la app muestra la información relacionada con la ciudad, el país y el código postal para calcular los gastos de envío finales. Sin embargo, no recibe toda la información solicitada hasta que el usuario autoriza el pago mediante Touch ID, Face ID o el código del dispositivo. Una vez autorizado, la información que se muestra en la hoja de Apple Pay se envía al beneficiario.

Cuando el usuario autoriza el pago, se envía un aviso a los servidores de Apple Pay para obtener un valor único criptográfico, que se parece al valor que devuelve el terminal NFC y que se utiliza para realizar transacciones en las tiendas. El valor único, junto con otros datos de la transacción, se transfiere al Secure Element para generar una credencial de pago que se encripta mediante una clave de Apple. Esta credencial de pago encriptada se transfiere del Secure Element a los servidores de Apple Pay, que la desencriptan, cotejan su valor único con el que ha enviado el Secure Element y la encriptan de nuevo con la clave del beneficiario asociada a su ID. Después, la credencial vuelve al dispositivo, que se encarga de devolverla a la app mediante la API. A continuación, la app se la facilita al sistema del beneficiario para que la procese. En ese momento, el beneficiario podrá desencriptar la credencial de pago con la ayuda de su clave privada para procesarla. Esto, en combinación con la firma de los servidores de Apple, permite que el beneficiario verifique que él es el destinatario de la transacción.

Las API requieren una autorización en la que se indiquen los ID compatibles del beneficiario. Al poder enviar también datos adicionales al Secure Element para que los firme como, por ejemplo, el número de pedido o la identidad del cliente, una app garantiza que la transacción no se pueda desviar a otro cliente. Esto lo lleva a cabo el desarrollador de la app, quien puede especificar applicationData en PKPaymentRequest. En los datos de pago encriptados, se incluye un hash de estos datos. A continuación, el beneficiario será responsable de verificar que su hash de applicationData coincida con el de los datos de pago.

Pagos con Apple Pay en la web o con Handoff

Apple Pay se puede utilizar para realizar pagos en sitios web. En iOS 10 o posterior, las transacciones de Apple Pay se pueden realizar en Internet en el iPhone y iPad. Además, en macOS Sierra o posterior, las transacciones de Apple Pay se pueden iniciar en una Mac y completarse en un iPhone compatible con Apple Pay, o un Apple Watch que utilice la misma cuenta de iCloud.

Apple Pay en la web requiere que todos los sitios web participantes se registren con Apple. Los servidores de Apple realizan la validación de nombres de dominio y emiten un certificado de cliente TLS. Los sitios web que soportan Apple Pay deben publicar su contenido a través de HTTPS. Para cada transacción de pago, los sitios web necesitan obtener una sesión de comerciante única y segura con un servidor Apple utilizando el certificado de cliente TLS emitido por Apple. Los datos de la sesión del comerciante están firmados por Apple. Una vez que se verifica la firma de una sesión de comerciante, un sitio web podría revisar si el usuario tiene un dispositivo compatible con Apple Pay y si tiene una tarjeta de crédito, débito o prepago activada en el dispositivo. No se comparte ninguna otra información. Si el usuario no desea compartir esta información, puede desactivar las consultas de Apple Pay en la configuración de privacidad de Safari en iOS y macOS.

Una vez que se valida una sesión de comerciante, todas las medidas de seguridad y privacidad son las mismas que cuando un usuario paga en una app.

En el caso de la transmisión mediante Handoff de Mac a iPhone o Apple Watch, Apple Pay utiliza el protocolo IDS encriptado de punto a punto para transmitir información relacionada con el pago entre la Mac del usuario y el dispositivo de autorización. IDS utiliza las claves de dispositivo del usuario para realizar el encriptado, por lo que ningún otro dispositivo puede desencriptar esta información y las claves no están disponibles para Apple. La detección de dispositivos para la función Handoff de Apple Pay contiene el tipo e identificador único de las tarjetas de crédito del usuario junto con algunos metadatos. El número de cuenta específico del dispositivo de la tarjeta del usuario no se comparte y se conserva almacenado de forma segura en el iPhone o Apple Watch del usuario. Apple también transfiere de forma segura las direcciones de contacto, envío y facturación usadas recientemente por el usuario a través del llavero de iCloud.

Una vez que el usuario autoriza el pago con Touch ID, Face ID o su código en el iPhone o presiona dos veces el botón lateral de Apple Watch, se envía de forma segura un identificador de pago encriptado único al certificado de comerciante de cada sitio web desde el iPhone o Apple Watch del usuario a la Mac y luego se envía al sitio web del comerciante.

Sólo los dispositivos cercanos pueden solicitar y completar el pago. La proximidad se determina a través de los anuncios de Bluetooth LE.

Tarjetas de recompensa

A partir de iOS 9 o posterior, Apple Pay es compatible con el protocolo de Servicio de Valor Añadido (VAS) para la transmisión de tarjetas de recompensa del beneficiario a terminales NFC compatibles. El protocolo VAS puede implementarse en las terminales del beneficiario y utiliza NFC para establecer la comunicación con dispositivos Apple compatibles. El protocolo VAS funciona a corta distancia y se utiliza para proporcionar servicios complementarios, como la transmisión de información de tarjetas de recompensa, como parte de una transacción de Apple Pay.

La terminal NFC inicia la recepción de la información de la tarjeta mediante el envío de una solicitud para dicha tarjeta. Si el usuario dispone de una tarjeta con el identificador de la tienda, se le solicitará que autorice su uso. Si el beneficiario permite la encriptación, se utilizan la información de la tarjeta, una fecha y una clave P-256 de ECDH aleatoria de un solo uso junto con la clave pública del beneficiario para derivar una clave de encriptación para los datos de la tarjeta, que se envían a la terminal. Si el beneficiario no permite la encriptación, se solicita al usuario que vuelva a presentar el dispositivo a la terminal antes de enviarse la información de la tarjeta de recompensa.

Apple Pay Cash

A partir de iOS 11.2 y watchOS 4.2, se puede usar Apple Pay en el iPhone, iPad, o Apple Watch para enviar, recibir o solicitar dinero a otros usuarios. Cuando un usuario recibe dinero, este se agrega a una cuenta de Apple Pay Cash a la cual se puede acceder desde Wallet o desde Configuración > "Wallet y Apple Pay" en cualquiera de los dispositivos elegibles en los que el usuario haya iniciado sesión con su Apple ID.

Para realizar pagos de usuario a usuario y Apple Pay Cash, el usuario debe haber iniciado sesión en su cuenta de iCloud en un dispositivo compatible con Apple Pay Cash, y debe tener la autenticación de dos factores configurada en la cuenta iCloud.

Al configurar Apple Pay Cash, se podría compartir con nuestro socio bancario Green Dot Bank y con Apple Payments Inc. la misma información que se proporciona cuando se agrega una tarjeta de crédito o débito. Apple Payments Inc. es una filial de propiedad exclusiva creada para proteger tu privacidad al almacenar y procesar información de manera independiente del resto de Apple y de una forma que el resto de Apple no conoce. Esta información sólo se utiliza para la solución de problemas, prevención del fraude y fines legislativos.

Las solicitudes y transferencias de dinero entre los usuarios se inician desde la app Mensajes o mediante una solicitud a Siri. Cuando un usuario intenta enviar dinero, iMessage muestra la hoja de Apple Pay. En todos los casos, primero se usa el saldo disponible en Apple Pay Cash. Si es necesario, se retiran fondos adicionales de una segunda tarjeta de crédito o débito que el usuario haya agregando a Wallet.

La tarjeta de Apple Pay Cash en Wallet se puede usar con Apple Pay para realizar pagos en las tiendas, apps y en Internet. El dinero disponible en Apple Pay Cash también se puede transferir a una cuenta bancaria. Además de recibir dinero de otro usuario, se puede agregar dinero a la cuenta Apple Pay Cash desde una tarjeta de débito o crédito en Wallet.

Apple Payments Inc. almacenará y podría usar los datos de tus transacciones para solucionar problemas, prevenir fraudes y para fines legislativos una vez que se complete la transacción. El resto de Apple no sabe a quién le enviaste dinero, quién te envió dinero, o dónde realizaste una compra con tu tarjeta Apple Pay Cash.

Cuando el usuario envía dinero con Apple Pay, agrega dinero a una cuenta de Apple Pay Cash, o transfiere dinero a una cuenta bancaria, se realiza una llamada a los servidores de Apple Pay para obtener un valor único criptográfico similar al valor obtenido para Apple Pay desde las apps. El valor único junto con otros datos de la transacción se transfiere al Secure Element para generar una firma de pago. Cuando la firma de pago sale del Secure Element, se pasa a los servidores de Apple Pay. Los servidores de Apple Pay verifican la autenticación, integridad y exactitud de la transacción mediante la firma de pago y el valor único. A continuación, se inicia la transferencia de dinero y se notifica al usuario cuando haya finalizado la transacción.

Si la transacción requiere una tarjeta de crédito o débito para:

- agregar dinero a Apple Pay Cash,
- enviar dinero a otro usuario o
- proporcionar dinero adicional si el saldo en Apple Pay Cash no es suficiente.

Entonces, además de la firma de pago descrita anteriormente, se produce una credencial de pago encriptada y se envía a los servidores de Apple Pay, similar a la que se crea para utilizar Apple Pay en apps y sitios web.

Cuando el saldo en la cuenta Apple Pay Cash supera un monto específico, o si se detecta alguna actividad inusual, se pide al usuario que verifique su identidad. La información que se proporciona para verificar la identidad de un usuario, tal como el número de seguro social o las respuestas a preguntas (por ejemplo, confirmar el nombre de la calle en la que solías vivir) se transmite de forma segura al socio de Apple y se encripta utilizando su clave. Apple no puede desencriptar estos datos.

Tarjetas Suica

En Japón, los usuarios pueden agregar una tarjeta Suica a Wallet de Apple Pay en los modelos de iPhone y Apple Watch compatibles. Esto se puede realizar mediante la transferencia del valor y el pase de transporte de una tarjeta física a su representación digital en Wallet, o agregando una nueva tarjeta Suica a Wallet desde la app de Suica. Después de agregar tarjetas Suica a Wallet, los usuarios pueden pagar en las tiendas o en el sistema de transporte público con su tarjeta anónima Suica, su tarjeta MySuica, o la tarjeta que contenga un pase de transporte.

Las tarjetas Suica se asocian con la cuenta iCloud del usuario. Si el usuario agrega más de una tarjeta a Wallet, Apple o el emisor de la tarjeta de transporte podrían enlazar la información personal del usuario y la información de la cuenta asociada entre las tarjetas; por ejemplo, las tarjetas MySuica se podrían enlazar con tarjetas anónimas Suica. Las tarjetas Suica y las transacciones están protegidas por un conjunto de claves criptográficas jerárquicas.

En el caso de una tarjeta Suica anónima, los usuarios deberán ingresar los últimos cuatro dígitos del número de serie de la tarjeta durante el proceso de transferencia de saldo de una tarjeta física a Wallet. En el caso de las tarjetas MySuica o tarjetas que contengan un pase de transporte, los

usuarios deberán ingresar también su fecha de nacimiento como prueba de posesión de la tarjeta. Al transferir pases desde un iPhone a un Apple Watch, ambos dispositivos deben estar conectados a Internet durante la transferencia.

Se puede recargar saldo utilizando tarjetas de crédito o prepago mediante Wallet o desde la app Suica. Los aspectos de la seguridad al recargar saldo utilizando Apple Pay se detallan en la sección "Pagos con Apple Pay desde apps" de este documento.

Para obtener información sobre cómo agregar la tarjeta Suica desde la app Suica, consulta la sección "Agregar tarjetas de crédito o débito desde la app de la entidad emisora de la tarjeta" de este documento.

El emisor de la tarjeta de transporte cuenta con las claves criptográficas necesarias para autenticar la tarjeta física y verificar los datos ingresados por el usuario. Después de completar la verificación, el sistema puede crear un número de cuenta del dispositivo para el Secure Element y activar el pase recién agregado en Wallet con el saldo transferido. Una vez que se haya transferido la información de la tarjeta de plástico, se desactivará la tarjeta física.

Al completar el proceso con cualquiera de estos métodos, el saldo Suica se encripta y almacena en un applet designado en el Secure Element. El operador de transporte tiene las claves para realizar operaciones criptográficas en los datos de la tarjeta para las transacciones de saldo.

De forma predeterminada, los usuarios se benefician de la experiencia intuitiva de Express Transit que les permite pagar y viajar sin requerir Touch ID, Face ID o un código. Es posible acceder a información, como estaciones visitadas recientemente, el historial de transacciones y la compra de boletos adicionales, en cualquier lector de tarjetas sin contacto cercano con el modo express activado. Para activar la solicitud de autorización mediante Touch ID, Face ID o código, se debe desactivar el abordaje exprés en Configuración > Wallet y Apple Pay.

Igual que con las tarjetas Apple Pay, los usuarios pueden suspender o eliminar tarjetas Suica de la siguientes formas:

- Al borrar el dispositivo de forma remota con "Buscar mi iPhone".
- Al activar el modo perdido con "Buscar mi iPhone".
- Al realizar operaciones de borrado remoto mediante MDM.
- Al eliminar todas las tarjetas de la página de su cuenta Apple ID.
- Al eliminar todas las tarjetas de iCloud.com.
- Al eliminar todas las tarjetas de Wallet.

Los servidores de Apple Pay solicitarán al operador de transporte que desactive las tarjetas Suica. Si el dispositivo no está conectado cuando se intente borrar, es posible que las tarjetas Suica aún se puedan usar en algunas terminales hasta las 12:01 a.m. JST del siguiente día.

Si los usuarios eliminan sus tarjetas Suica, es posible recuperar el saldo. Los usuarios podrán volver a agregarlas a un dispositivo donde hayan iniciado sesión con el mismo Apple ID después de las 5:00 a.m. JST del siguiente día.

No podrás suspender las tarjetas Suica si tu dispositivo no tiene conexión.

Suspensión, eliminación y borrado de tarjetas

Los usuarios pueden suspender el servicio Apple Pay en el iPhone, iPad y Apple Watch con watchOS 3, al activar el modo perdido en sus dispositivos mediante "Buscar mi iPhone". Los usuarios también tienen la posibilidad de eliminar y borrar sus tarjetas de Apple Pay utilizando "Buscar mi iPhone", iCloud.com, o bien directamente en sus dispositivos mediante Wallet. En el Apple Watch, las tarjetas se pueden eliminar mediante la configuración de iCloud, la app Apple Watch del iPhone, o bien directamente en el reloj. La entidad emisora de la tarjeta o la red de pago correspondiente suspenderá o eliminará la posibilidad de realizar pagos mediante las tarjetas del dispositivo con Apple Pay, aunque el dispositivo no esté en línea ni conectado a una red de datos celular o Wi-Fi. Los usuarios también pueden llamar a la entidad emisora de la tarjeta para suspender o eliminar tarjetas de Apple Pay.

Además, cuando un usuario borre todo el dispositivo utilizando la opción "Borrar todo el contenido y configuración", desde "Buscar mi iPhone" o restaurándolo en el modo de recuperación, iOS le indicará a Secure Element que marque todas las tarjetas como eliminadas. El resultado inmediato es que las tarjetas dejan de poder utilizarse hasta que se pueda establecer contacto con los servidores de Apple Pay para solicitarles que eliminen las tarjetas del Secure Element por completo. Independientemente, el Secure Enclave marca el valor AR como no válido para impedir cualquier autorización de pago con las tarjetas registradas previamente. Cuando el dispositivo está en línea, intenta ponerse en contacto con los servidores de Apple Pay para cerciorarse de que todas las tarjetas se hayan borrado del Secure Element.

Servicios de Internet

Cómo crear contraseñas de Apple ID seguras
Los Apple ID se utilizan para permitir la conexión a una serie de servicios, entre los que se incluyen iCloud, FaceTime y iMessage. Con el objetivo de ayudar a los usuarios a crear contraseñas seguras, todas las contraseñas de las cuentas nuevas deben contener los siguientes atributos:

- Al menos ocho caracteres
- Al menos una letra
- Al menos una letra mayúscula
- Al menos un número
- No más de tres caracteres idénticos consecutivos
- No debe coincidir con el nombre de la cuenta

Apple creó un robusto conjunto de servicios para ayudar a los usuarios a aprovechar todavía más la utilidad y productividad de sus dispositivos. Estos servicios incluyen iMessage, FaceTime, las sugerencias de Siri, iCloud, el respaldo de iCloud y el llavero de iCloud.

Estos servicios de Internet están diseñados con los mismos objetivos de seguridad que iOS promueve en toda su plataforma. Dichos objetivos incluyen la administración segura de datos, tanto si no se están utilizando en el dispositivo como si se están transfiriendo por redes inalámbricas; la protección de la información personal de los usuarios; y la protección frente al acceso malintencionado o no autorizado a la información y los servicios. Cada servicio utiliza su propia arquitectura de seguridad sin afectar la facilidad de uso de iOS.

Apple ID

El Apple ID es la cuenta necesaria para iniciar sesión en servicios de Apple tales como iCloud, iMessage, FaceTime, iTunes Store, iBooks Store, App Store, entre otros. Es importante que los usuarios protejan su Apple ID para evitar que se produzca un acceso no autorizado a sus cuentas. Con el fin de ayudarles a conseguirlo, Apple exige el uso de contraseñas seguras compuestas de al menos ocho caracteres que combinen números y letras, que no contengan el mismo carácter repetido más de tres veces de forma consecutiva y que no sean de uso común. Se recomienda a los usuarios que aumenten el grado de protección indicado agregando más caracteres o signos de puntuación para que sus contraseñas resulten aún más seguras. Apple también solicita al usuario que defina tres preguntas de seguridad que pueden usarse para ayudar a verificar la identidad del propietario al momento de realizar cambios en la información de la cuenta o al restablecer una contraseña olvidada.

Apple también envía mensajes de correo electrónico y notificaciones push a los usuarios cuando se producen cambios importantes en sus cuentas. Por ejemplo, si se modifica una contraseña o la información de facturación, o bien si el Apple ID se usa para iniciar sesión en un dispositivo nuevo. Si los usuarios detectan algo que no les resulta familiar, deben cambiar la contraseña de su Apple ID inmediatamente.

Además, Apple usa una variedad de políticas y procedimientos diseñados para proteger las cuentas de los usuarios. Estos incluyen limitar las veces que se pueden reingresar los datos de inicio de sesión o restablecer la contraseña, el monitoreo activo de fraude para identificar ataques en el momento en el que ocurran, y revisiones periódicas de las políticas que permiten a Apple adaptarse a cualquier información nueva que pueda afectar la seguridad del cliente.

Autenticación de dos factores

Para ayudar a los usuarios a proteger sus cuentas, Apple ofrece la *autenticación de dos factores*, una capa de seguridad adicional para los Apple ID. Está diseñada para asegurar que sólo el propietario de la cuenta pueda acceder a la misma, incluso si alguien más conoce la contraseña.

Con la autenticación de dos factores, la cuenta de un usuario se puede acceder sólo en dispositivos de confianza, tales como el iPhone, iPad o Mac del usuario. Para iniciar sesión por primera vez en cualquier dispositivo nuevo, se necesitan dos datos: la contraseña del Apple ID y un código de verificación de seis dígitos que se muestra automáticamente en los dispositivos de confianza del usuario o que se envía a un número telefónico de confianza. Al ingresar este código, el usuario verifica que confía en el nuevo dispositivo y que es seguro iniciar sesión. Dado que una contraseña por sí misma no es suficiente para acceder a la cuenta del usuario, la autenticación de dos factores mejora la seguridad del Apple ID del usuario y de toda la información personal que almacene con Apple. Viene integrada directamente en iOS, macOS, tvOS, watchOS y los sistemas de autenticación usados en los sitios web de Apple.

Para obtener más información sobre la autenticación de dos factores, consulta: https://support.apple.com/es-lamr/HT204915.

Verificación en dos pasos

Desde 2013, Apple también ofrece un método de seguridad similar llamado *verificación en dos pasos*. Con la verificación en dos pasos activada, la identidad del usuario se debe comprobar mediante un código temporal que se envía a uno de los dispositivos de confianza del usuario antes de permitir algún cambio en la información de la cuenta de su Apple ID, antes de iniciar sesión en iCloud, iMessage, FaceTime o Game Center, o antes de realizar compras en iTunes Store, iBooks Store o App Store desde un dispositivo nuevo. Los usuarios también reciben una clave de recuperación de 14 caracteres que deben guardar en un lugar seguro para usarla en caso de olvidar su contraseña o perder el acceso a los dispositivos de confianza. A pesar de que se recomienda la autenticación de dos factores a la mayoría de los usuarios nuevos, hay algunas situaciones en las que se recomienda la verificación en dos pasos.

Para obtener más información sobre la verificación en dos pasos del Apple ID, consulta: https://support.apple.com/es-lamr/ht5570.

Apple ID administrados

Los Apple ID administrados funcionan de manera similar a un Apple ID, pero se trata de cuentas que son propiedad de una institución educativa, que es la que los controla. La institución puede restablecer contraseñas, limitar las compras y las comunicaciones, tales como FaceTime y Mensajes, y configurar permisos basados en roles para profesores, estudiantes y el resto del personal.

Algunos servicios de Apple están desactivados en los Apple ID administrados, tales como Apple Pay, el llavero de iCloud, HomeKit y Buscar mi iPhone.

Para obtener más información sobre los Apple ID administrados, consulta: https://help.apple.com/schoolmanager/.

Auditar Apple ID administrados

Los Apple ID administrados se pueden auditar, lo que permite a las instituciones cumplir con las regulaciones legales y de privacidad. Las cuentas de administrador, director o profesor pueden obtener privilegios de auditoría para Apple ID administrados específicos. Los auditores sólo pueden monitorear las cuentas que estén por debajo de su posición jerárquica en la escuela. Eso significa que los profesores pueden monitorear estudiantes; los directivos pueden auditar profesores y estudiantes; y los administradores pueden auditar a los directivos, profesores y estudiantes.

Cuando se solicitan credenciales de auditoría mediante Apple School Manager, se crea una cuenta especial que tiene acceso sólo a los Apple ID administrados para los cuales se solicitó auditoría. Los permisos de auditoría caducan después de siete días. Durante este periodo, el auditor puede leer y modificar el contenido del usuario almacenado en iCloud o en apps con CloudKit activado. Cada solicitud de acceso de auditoría se registra en Apple School Manager. El registro muestra quién fue el auditor, el Apple ID administrado al que se solicitó acceso, la hora de la solicitud y si se realizó la auditoría.

Apple ID administrados y dispositivos personales

Los Apple ID administrados también se pueden usar en dispositivos iOS y computadoras Mac personales. Los estudiantes pueden iniciar sesión en iCloud usando un Apple ID administrado proporcionado por la institución y una contraseña adicional de uso particular que funge como segundo factor en el proceso de autenticación de dos factores del Apple ID. Al usar un Apple ID administrado en un dispositivo personal, el llavero de iCloud no está disponible, y la institución podría restringir otras funciones, tales como FaceTime o Mensajes. Todos los documentos de iCloud creados por estudiantes mientras tengan iniciada la sesión están sujetos a auditoría de la manera previamente descrita en esta sección.

iMessage

iMessage de Apple es un servicio de mensajería para dispositivos iOS, Apple Watch y computadoras Mac. iMessage admite texto y archivos adjuntos tales como fotos, contactos y ubicaciones. Puesto que los mensajes se muestran en todos los dispositivos registrados de un usuario, una conversación se puede continuar desde cualquiera de sus dispositivos. iMessage utiliza el servicio de notificaciones push de Apple (APNs) en gran medida. Apple no registra el contenido de los mensajes o archivos adjuntos, los cuales están protegidos mediante una encriptación de punto a punto, de modo que únicamente el emisor y el receptor pueden acceder a ellos. Apple no puede desencriptar los datos.

Cuando un usuario activa iMessage en un dispositivo, el dispositivo genera dos pares de claves para usarlas con el servicio: una clave RSA de 1280 bits para la encriptación y una clave ECDSA de 256 bits en la curva P-256 del NIST para el inicio de sesión. Las claves privadas de ambos pares de claves se guardan en el llavero del dispositivo y las claves públicas se envían al servicio de directorio (IDS) de Apple, donde se asocian al número de teléfono o la dirección de correo electrónico del usuario, junto con la dirección del servicio APNs del dispositivo.

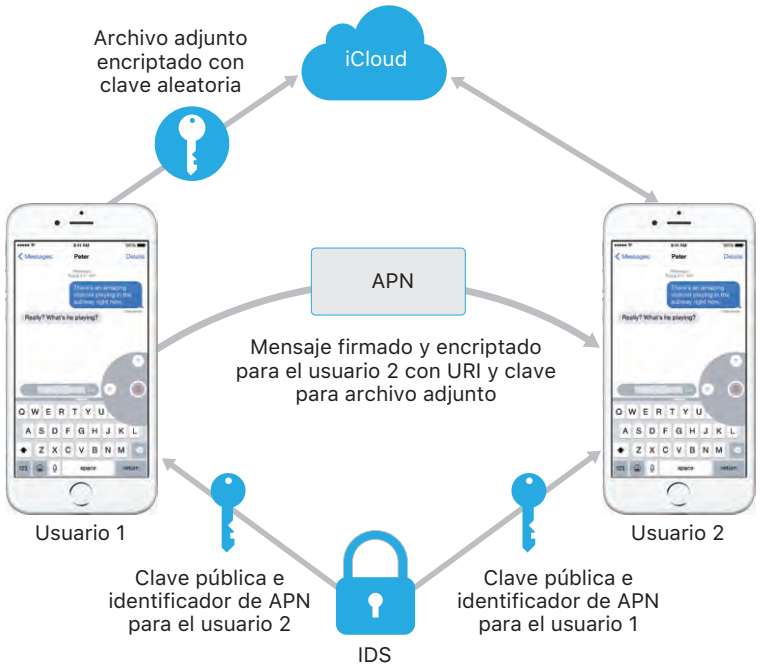
A medida que los usuarios activan otros dispositivos para usarlos con iMessage, las claves públicas de encriptación y firma, las direcciones del APNs y los números de teléfono asociados se agregan al servicio de directorio. Los usuarios también pueden agregar más direcciones de correo electrónico, que se verifican mediante el envío de un enlace de confirmación. La SIM y la red del operador verifican los números de teléfono. En algunas redes, esto requiere el uso de SMS (aparecerá un cuadro de diálogo de confirmación en el caso de que el SMS no sea gratuito). Además de iMessage, varios servicios del sistema, como FaceTime y iCloud, podrían requerir la verificación del número telefónico. Todos los dispositivos registrados del usuario muestran un mensaje de aviso al agregar un dispositivo, número de teléfono o dirección de correo electrónico nuevos.

Cómo iMessage envía y recibe mensajes

Los usuarios inician una nueva conversación de iMessage al ingresar una dirección o un nombre. Si ingresan un número de teléfono o una dirección de correo electrónico, el dispositivo se pone en contacto con el IDS para recuperar las claves públicas y las direcciones del APNs de todos los dispositivos asociados al destinatario. Si el usuario ingresa un nombre, el dispositivo utiliza primero la app Contactos del usuario para recopilar los números de teléfono y las direcciones de correo electrónico asociadas a ese nombre, y luego obtiene las claves públicas y las direcciones del APNs del IDS.

El mensaje que envía el usuario está encriptado de forma individual para cada uno de los dispositivos del destinatario. Las claves de encriptación RSA públicas de los dispositivos receptores se obtienen del IDS. Para cada dispositivo receptor, el dispositivo emisor genera un valor aleatorio de 88 bits y lo utiliza como una clave HMAC-SHA256 para construir un valor de 40 bits derivado de la clave pública del emisor y del receptor y del texto sin formato. La concatenación de los valores de 88 bits y 40 bits hace una clave de 128 bits, que encripta el mensaje usando AES en modo CTR. El receptor usa el valor de 40 bits para verificar la integridad del texto sin formato desencriptado. Esta clave AES por mensaje se encripta con RSA-OAEP para la clave pública del dispositivo receptor. Con el texto del mensaje encriptado y la clave del mensaje encriptada se genera un hash SHA-1, que se firma con ECDSA utilizando la clave de firma privada del dispositivo emisor. Los mensajes que se obtienen, uno para cada dispositivo receptor, están constituidos por el texto del mensaje encriptado, la clave del mensaje encriptada y la firma digital del emisor. A continuación, se mandan al APNs para que los envíe. Los metadatos, como la fecha y la información sobre el enrutamiento del APNs, no se encriptan. La comunicación con el APNs se encripta utilizando un canal TLS de secreto-hacia-delante.

El APNs sólo puede transmitir mensajes de 4 KB ó 16 KB como máximo en función de la versión de iOS. Si el texto del mensaje es demasiado largo o si se incluye un archivo adjunto (por ejemplo, una foto), el archivo adjunto se encripta con AES en modo CTR utilizando una clave de 256 bits generada aleatoriamente, y se carga a iCloud. Después, la clave AES para el archivo adjunto, su identificador de recursos uniforme (URI) y un hash SHA-1 de su forma encriptada se envían al destinatario como el contenido de un mensaje de iMessage, cuya confidencialidad e integridad están protegidas mediante la encriptación normal de iMessage, como se muestra en el siguiente diagrama.



En el caso de las conversaciones de grupo, este proceso se repite para cada destinatario y sus dispositivos.

En cuanto a la recepción, cada dispositivo recibe una copia del mensaje desde el APNs y, en caso de ser necesario, obtiene el archivo adjunto de iCloud. El número de teléfono o la dirección de correo electrónico del emisor del mensaje se cotejan con los contactos del receptor para que, cuando sea posible, se muestre el nombre.

Como sucede con todas las notificaciones push, el mensaje se elimina del APNs una vez enviado. Sin embargo, a diferencia de lo que sucede con otras notificaciones del APNs, los mensajes de iMessage se ponen en cola para enviarlos a los dispositivos sin conexión. Actualmente, los mensajes se almacenan durante un plazo máximo de 30 días.

FaceTime

FaceTime es el servicio de llamadas de audio y video de Apple. De forma parecida a iMessage, las llamadas de FaceTime también utilizan el servicio de notificaciones push de Apple para establecer una conexión inicial con los dispositivos registrados del usuario. El contenido de audio/video de las llamadas FaceTime se protege mediante la encriptación de punto a punto, así que únicamente el emisor y el receptor pueden acceder a él, Apple no puede desencriptar los datos.

La conexión inicial de FaceTime se realiza a través de la estructura de servidores de Apple que retransmite los paquetes de datos entre los dispositivos registrados del usuario. Al usar notificaciones APNs y mensajes con Utilidades Transversales de Sesión para NAT (STUN) a través de la conexión retransmitida, los dispositivos verifican sus certificados de identidad y establecen un secreto compartido para cada sesión. El secreto compartido se usa para derivar las claves por sesión para canales de contenido que se transmiten vía el Protocolo de transporte en tiempo real seguro (SRTP). Los paquetes del SRTP se encriptan utilizando AES-256 en el modo Counter y HMAC-SHA1. Después de la conexión inicial y la

configuración de seguridad, FaceTime utiliza STUN y el Establecimiento de la conexión a Internet (ICE) para establecer una conexión P2P entre los dispositivos, si es posible.

iCloud

iCloud almacena los contactos, calendarios, fotos, documentos y otra información del usuario, y la mantiene al día automáticamente en todos sus dispositivos. Además, las apps de terceros también pueden usar iCloud para almacenar y sincronizar documentos, así como datos clave-valor para datos de apps según las indicaciones del desarrollador. Los usuarios configuran iCloud al iniciar sesión con un Apple ID y seleccionar qué servicios desean usar. Los administradores de TI pueden desactivar funciones de iCloud tales como "Secuencias de fotos", iCloud Drive y el respaldo de iCloud mediante perfiles de configuración MDM. El servicio no reconoce qué se está almacenando y administra el contenido de los archivos de la misma forma: como un conjunto de bytes.

iCloud encripta cada archivo, que se desglosa en fragmentos, con AES-128 y una clave derivada del contenido de cada fragmento que utiliza SHA-256. Apple almacena las claves y los metadatos de los archivos en la cuenta de iCloud del usuario. Los fragmentos encriptados del archivo se almacenan (sin incluir información que pudiera divulgar la identidad del usuario) mediante servicios de almacenamiento de terceros como S3 y Google Cloud Platform.

iCloud Drive

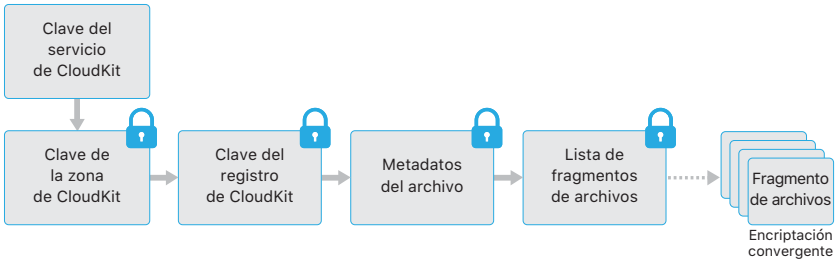
iCloud Drive agrega claves basadas en las cuentas para proteger los documentos almacenados en iCloud. Tal como sucede con los servicios de iCloud existentes, este servicio fragmenta y encripta el contenido de los archivos y almacena los fragmentos encriptados mediante servicios de terceros. Sin embargo, las claves de contenido de los archivos están encapsuladas en claves de registro almacenadas junto con los metadatos de iCloud Drive. La clave de servicio de iCloud Drive del usuario protege esas claves de registro; y dicha clave de servicio se almacena con la cuenta de iCloud del usuario. Después de autenticarse con iCloud, los usuarios pueden acceder a los metadatos de los documentos de iCloud, pero también necesitan la clave de servicio de iCloud Drive para que se muestren las secciones protegidas del almacenamiento de iCloud Drive.

CloudKit

CloudKit permite a los desarrolladores de apps almacenar datos de clave-valor, datos estructurados y componentes en iCloud. El acceso a CloudKit se controla con las autorizaciones de la app. CloudKit es compatible con bases de datos tanto públicas como privadas. Todas las copias de la app usan bases de datos públicas, normalmente para los componentes generales, y no están encriptadas. En las bases de datos privadas, se almacenan los datos del usuario.

Igual que iCloud Drive, CloudKit utiliza claves basadas en las cuentas para proteger la información almacenada en la base de datos privada del usuario y, como sucede en otros servicios de iCloud, los archivos se fragmentan, se encriptan y se almacenan usando servicios de terceros. CloudKit usa una jerarquía de claves parecida a la de la protección de datos. Las claves por archivo se encapsulan en claves de registro de CloudKit. Estas últimas están protegidas por una clave de zona amplia, que a su vez está protegida

mediante la clave de servicio de CloudKit. La clave de servicio de CloudKit se almacena en la cuenta de iCloud del usuario y sólo está disponible una vez que el usuario se ha autenticado con iCloud.



Encriptación de punto a punto de CloudKit

Apple Pay Cash, las palabras clave del usuario, la inteligencia de Siri y Oye Siri usan encriptación de punto a punto de CloudKit con una clave de servicio de CloudKit protegida por la sincronización del llavero de iCloud. En el caso de estos contenedores de CloudKit, la jerarquía de las claves está integrada en el llavero de iCloud, de modo que comparte sus características de seguridad. Las claves están disponibles sólo en los dispositivos de confianza del usuario, y ni Apple ni terceras partes pueden acceder a ellas. Si se pierde el acceso a los datos del llavero de iCloud (consulta la sección "Seguridad de la custodia" más adelante en este documento), se restablecen los datos en CloudKit y, si hay datos disponibles en el dispositivo local de confianza, se vuelven a cargar a CloudKit.

Respaldo de iCloud

iCloud también realiza respaldos de información (como configuración de los dispositivos, datos de las apps, fotos y videos en "Rollo fotográfico", así como conversaciones en la app Mensajes) a diario y a través de la red Wi-Fi. Para proteger el contenido, iCloud lo encripta cuando se envía por Internet, lo almacena en un formato encriptado y utiliza identificadores seguros para su autenticación. Los respaldos de iCloud se llevan a cabo únicamente cuando el dispositivo está bloqueado, conectado a una fuente de alimentación y tiene acceso a Internet mediante Wi-Fi. Debido a la encriptación que se usa en iOS, el sistema está diseñado para mantener protegidos los datos y, al mismo tiempo, permitir que se realicen respaldos y restauraciones progresivas y sin supervisión.

iCloud realiza respaldos del contenido siguiente:

- Registros de música, películas, programas de TV, apps y libros comprados. El respaldo de iCloud de un usuario incluye información sobre el contenido comprado presente en el dispositivo iOS, pero no contiene el contenido comprado en sí. Cuando el usuario realiza una restauración a partir de un respaldo de iCloud, su contenido comprado se descarga automáticamente desde iTunes Store, App Store o iBooks Store. Algunos tipos de contenido no se descargan automáticamente en todos los países, y las compras previas podrían no estar disponibles si se han reembolsado o si ya no están disponibles en la tienda. El historial de compras completo está asociado al Apple ID del usuario.
- Fotos y videos en un dispositivo del usuario. Ten en cuenta que si el usuario activa la fototeca de iCloud en su dispositivo iOS (con iOS 8.1 o posterior) o Mac (OS X 10.10.3 o posterior), sus fotos y videos ya se almacenan en iCloud, por lo que no se incluyen en su respaldo de iCloud.
- Contactos, eventos de calendario, recordatorios y notas.

- Configuración del dispositivo.
- Datos de apps.
- Historial de llamada y tonos de llamada.
- Organización de la pantalla de inicio y las apps.
- Configuración de HomeKit.
- Datos de HealthKit.
- iMessage, mensajes de texto (SMS) y mensajes MMS (requiere la tarjeta SIM que se usó durante el respaldo).
- Contraseña del buzón de voz visual (requiere la tarjeta SIM que se usó durante el respaldo).

Cuando los archivos se crean en clases de protección de datos a las que no se puede acceder cuando el dispositivo está bloqueado, las claves por archivo correspondientes se encriptan con las claves de clase del depósito de claves de respaldo de iCloud. Los respaldos en iCloud de los archivos se realizan en su estado encriptado original. Los archivos de la clase de protección de datos "Sin protección" se encriptan durante el transporte.

El depósito de claves de respaldo de iCloud contiene claves asimétricas (Curve25519) para cada clase de protección de datos. Estas claves asimétricas se usan para encriptar las claves por archivo. Para obtener más información acerca del contenido de claves de respaldo y de respaldo de iCloud, consulta el apartado "Protección de datos de llavero" de la sección "Encriptación y protección de datos".

El conjunto de respaldos se almacena en la cuenta de iCloud del usuario y consiste en una copia de los archivos del usuario y el depósito de claves de respaldo de iCloud. Este depósito está protegido mediante una clave aleatoria, que también está almacenada en el conjunto de respaldos (la contraseña de iCloud del usuario no se usa para la encriptación; de este modo, el cambio de contraseña de iCloud no invalida los respaldos existentes).

Mientras se mantenga una copia de la base de datos del llavero del usuario en iCloud, ésta permanecerá protegida mediante una clave vinculada al UID. Esto permite que el llavero sólo se pueda restaurar en el mismo dispositivo en el que se originó; es decir que nadie más (incluido Apple) puede leer los elementos del llavero del usuario.

Al restaurarlo, se recuperan de la cuenta de iCloud del usuario los archivos de los que se ha realizado un respaldo, el depósito de claves de respaldo de iCloud y la clave para el depósito de claves. El depósito de claves del respaldo de iCloud se desencripta usando su clave, luego las claves por archivo del depósito de claves se usan para desencriptar los archivos del conjunto de respaldos, que se escriben como archivos nuevos en el sistema de archivos y, de este modo, se vuelven a encriptar según la clase de protección de datos correspondiente.

Integración de Safari con el llavero de iCloud
Safari puede generar automáticamente cadenas aleatorias seguras criptográficamente para las contraseñas de los sitios web, las cuales se almacenan en el llavero y se sincronizan con otros dispositivos. Los elementos del llavero se transfieren de un dispositivo a otro a través de los servidores de Apple. Sin embargo, están encriptados de manera que ni Apple ni otros dispositivos pueden leer su contenido.

Llavero de iCloud

El llavero de iCloud permite a los usuarios sincronizar de manera segura sus contraseñas entre sus dispositivos iOS y computadoras Mac sin revelar su información a Apple. Además de un alto grado de privacidad y seguridad, existen otros objetivos que han influido notablemente en el diseño y la arquitectura del llavero de iCloud como, por ejemplo, su facilidad de uso y la posibilidad de recuperarlo. El llavero de iCloud consta de dos servicios: la sincronización del llavero y su recuperación.

Apple diseñó el llavero de iCloud y la recuperación del mismo para que las contraseñas del usuario se mantuvieran protegidas en las siguientes circunstancias:

- Si se violó la seguridad de la cuenta de iCloud de un usuario.
- Si se violó la seguridad de iCloud a causa de un ataque externo o de un empleado.
- Si un tercero accedió a las cuentas del usuario.

Sincronización del llavero

Cuando un usuario activa el llavero de iCloud por primera vez, el dispositivo establece un círculo de confianza y crea una identidad de sincronización para sí mismo. La identidad de sincronización consta de una clave privada y una clave pública. La clave pública de la identidad de sincronización se coloca en el círculo y el círculo se firma dos veces: primero, lo firma la clave privada de la identidad de sincronización y, después, una clave de curva elíptica asimétrica (con P-256) derivada de la contraseña de la cuenta de iCloud del usuario. Junto con el círculo, se almacenan los parámetros (sal aleatoria e iteraciones), usados para crear la clave que se basa en la contraseña de iCloud del usuario.

El círculo de sincronización firmado se ubica en el área de almacenamiento de datos clave-valor de iCloud del usuario. No se puede leer sin conocer la contraseña de iCloud del usuario y no se puede modificar de forma válida sin disponer de la clave privada de la identidad de sincronización de su miembro.

Cuando el usuario activa el llavero de iCloud en otro dispositivo, este detecta que el usuario dispone de un círculo de sincronización en iCloud previamente establecido al cual el dispositivo no pertenece. El dispositivo crea el par de claves de identidad de sincronización correspondiente y luego crea un ticket de aplicación para solicitar formar parte de ese círculo como miembro. El ticket consta de la clave pública del dispositivo de su identidad de sincronización, y se solicita al usuario que se autentique con su contraseña de iCloud. Los parámetros de generación de la clave de curva elíptica se obtienen de iCloud y se genera una clave que se usa para firmar el ticket de aplicación. Por último, este ticket se coloca en iCloud.

Cuando el primer dispositivo detecta la recepción de un ticket de aplicación, muestra un aviso para que el usuario sepa que hay un dispositivo nuevo que solicita entrar en el círculo de sincronización. El usuario ingresa su contraseña de iCloud, y se comprueba que el ticket de aplicación esté firmado por una clave privada coincidente. Esto determina que la persona que ha generado la solicitud para unirse al círculo ingresó la contraseña de iCloud del usuario cuando se le solicitó.

Después de la aprobación del usuario para agregar un dispositivo nuevo al círculo, el primer dispositivo agrega la clave pública del nuevo miembro al círculo de sincronización, y vuelve a firmarlo con la identidad de sincronización correspondiente y la clave derivada de la contraseña de iCloud del usuario. El nuevo círculo de sincronización se ubica en iCloud, donde el nuevo miembro lo firma de manera similar.

Así, el círculo de sincronización tiene dos miembros y cada uno de ellos dispone de la clave pública del otro. Estos empiezan a intercambiar elementos individuales del llavero mediante el almacenamiento de datos clave-valor de iCloud o a almacenarlos en CloudKit según sea necesario. Si ambos miembros del círculo disponen del mismo elemento, se sincronizará el de la fecha de modificación más reciente. Los elementos se ignorarán en el caso de que el otro miembro también los tenga con la misma fecha de modificación. Cada elemento sincronizado se encripta a fin de que sólo pueda ser desencriptado en un dispositivo perteneciente al círculo de confianza del usuario. Ni Apple ni otros dispositivos pueden desencriptarlo.

Este proceso se repite cada vez que se unen nuevos dispositivos al círculo de sincronización. Por ejemplo, si se une un tercer dispositivo, la confirmación se muestra en los otros dos dispositivos del usuario. El usuario puede aprobar la incorporación del nuevo miembro desde cualquiera de esos dispositivos. Al agregar nuevos dispositivos, cada uno se sincroniza con el nuevo para garantizar que todos los miembros disponen de los mismos elementos en el llavero.

Sin embargo, no se sincroniza todo el llavero. Algunos elementos, como las identidades de VPN, son específicos de cada dispositivo y no deben abandonarlo. Sólo se sincronizan los elementos con el atributo `kSecAttrSynchronizable`. Apple ha configurado este atributo para los datos de usuario de Safari (que incluyen los nombres de usuario, contraseñas y números de tarjetas de crédito), así como para las contraseñas de redes Wi-Fi y las claves de encriptación de HomeKit.

Además, de forma predeterminada, los elementos del llavero que hayan agregado apps de terceros no se sincronizan. Los desarrolladores deben definir el atributo `kSecAttrSynchronizable` al agregar elementos al llavero.

Recuperación del llavero

La recuperación del llavero ofrece a los usuarios la posibilidad de que Apple custodie su llavero, pero sin permitir que lea sus contraseñas u otros datos que contenga. Incluso si el usuario solamente dispone de un dispositivo, la recuperación del llavero le proporciona una red de seguridad frente a la pérdida de datos. Esto es especialmente importante cuando Safari se usa para generar contraseñas seguras y aleatorias para cuentas web, ya que el único registro de esas contraseñas está en el llavero.

Dos de los conceptos básicos de la recuperación del llavero son la autenticación secundaria y el servicio de custodia segura, ambos creados por Apple específicamente para admitir esta función. El llavero del usuario se encripta mediante un código seguro, y el servicio de custodia proporciona una copia del llavero únicamente si se cumple una serie de condiciones estrictas.

Si la autenticación de dos factores está activada en la cuenta del usuario al momento de activar el llavero de iCloud, se usará el código del dispositivo para recuperar un llavero en custodia. Si no está activada la autenticación de dos factores, se le pide al usuario que cree un código de seguridad de iCloud utilizando un código de seis dígitos. De forma

opcional, sin la autenticación de dos factores, los usuarios pueden especificar su propio código, que puede ser más largo, o bien permitir que sus dispositivos generen un código aleatorio criptográfico, que pueden registrar y guardar.

A continuación, el dispositivo iOS exporta una copia del llavero del usuario, la encripta encapsulada con claves en un depósito de claves asimétrico y la coloca en el área de almacenamiento de datos clave-valor de iCloud del usuario. El depósito de claves se encapsula con el código de seguridad de iCloud del usuario y la clave pública del clúster del módulo de seguridad de hardware (HSM), que almacenará el registro de la custodia, convirtiéndose así en el registro de la custodia de iCloud del usuario.

Si el usuario decide aceptar un código de seguridad criptográficamente aleatorio en lugar de especificar el propio o utilizar un valor de cuatro dígitos, el registro de la custodia no será necesario, puesto que el código de seguridad de iCloud se utilizará para encapsular directamente la clave aleatoria.

Además de establecer un código de seguridad, el usuario debe registrar un número de teléfono. Esto proporciona un nivel secundario de autenticación durante la recuperación del llavero. El usuario recibirá un SMS al que debe responder para que se proceda a la recuperación.

Seguridad de la custodia

iCloud proporciona una infraestructura segura para custodias de llaveros, que garantiza que sólo los usuarios y los dispositivos autorizados puedan realizar una recuperación. Hay clústeres HSM posicionados topográficamente detrás de iCloud que guardan los registros de la custodia. Cada uno tiene una clave que sirve para encriptar los registros de la custodia bajo su supervisión, tal como se describió anteriormente en este documento.

Para recuperar el llavero, los usuarios deben autenticarse con su cuenta de iCloud y su contraseña, y deben responder a un SMS que se envía al teléfono que hayan registrado. Una vez hecho esto, los usuarios deben ingresar su código de seguridad de iCloud. El clúster HSM utiliza el protocolo de contraseña remota segura (SRP) para verificar que un usuario sabe el código de seguridad de iCloud; el código en sí no se envía a Apple. Cada miembro del clúster verifica de manera independiente que el usuario no haya superado el número máximo de intentos permitidos para recuperar el registro, como se indica a continuación. Si la mayoría está de acuerdo, el clúster desencapsula el registro de la custodia y lo envía al dispositivo del usuario.

A continuación, el dispositivo usa el código de seguridad de iCloud para desencapsular la clave aleatoria que se ha usado para encriptar el llavero del usuario. Con esa clave, el llavero, que se ha recuperado del almacenamiento de datos clave-valor de iCloud, se desencripta y se restaura en el dispositivo. Sólo se permiten 10 intentos para autenticar y recuperar un registro de la custodia. Después de varios intentos fallidos, el registro se bloquea y el usuario debe ponerse en contacto con el servicio de soporte de Apple para que se le concedan más intentos. Después del décimo intento fallido, el clúster del HSM destruye el registro de la custodia y el llavero se pierde para siempre. Este sistema ofrece protección frente a un intento de ataque de fuerza bruta para recuperar el registro aunque conlleve el sacrificio de los datos del llavero.

Estas políticas se codifican en el firmware del HSM. Las tarjetas de acceso administrativo que permiten que el firmware se modifique se han destruido. Cualquier intento de alterar el firmware o de acceder a la clave privada provocará que el clúster del HSM elimine dicha clave. Si esto sucede, el propietario de cada llavero que protege el clúster recibirá un mensaje en el que se indicará que se perdió el registro de la custodia. A continuación, podrán decidir si desean volver a inscribirse.

Siri

Los usuarios pueden utilizar Siri para enviar mensajes, organizar reuniones y hacer llamadas telefónicas, entre otras cosas, hablándole de forma natural. Siri utiliza el reconocimiento de voz, la conversión de texto a voz y un modelo cliente-servidor para responder a una amplia variedad de solicitudes. Las tareas que Siri admite están diseñadas para garantizar que solamente se utilice la cantidad mínima de información personal y que esté completamente protegida.

Cuando Siri se activa, el dispositivo crea identificadores aleatorios para usar con el reconocimiento de voz y los servidores de Siri. Estos identificadores se usan únicamente dentro de Siri y sirven para mejorar el servicio. Si después Siri se desactiva, el dispositivo genera un identificador aleatorio nuevo para usarlo cuando se vuelva a activar.

Para facilitar las funciones de Siri, parte de la información del usuario se envía del dispositivo al servidor. Esta incluye información acerca de la biblioteca musical (títulos de canciones, artistas y listas de reproducción), los nombres de las listas de Recordatorios, así como los nombres y las relaciones definidas en Contactos. Todas las comunicaciones con el servidor se realizan mediante el protocolo HTTPS.

Cuando se inicia una sesión de Siri, se envía al servidor el nombre y apellido del usuario (disponibles en Contactos), junto con una ubicación aproximada. Esto permite que Siri responda con el nombre o que responda a preguntas que sólo requieran una ubicación aproximada, por ejemplo, las relacionadas con el clima.

En caso de necesitar una ubicación más precisa, por ejemplo, para determinar la ubicación de un cine cercano, el servidor solicita al dispositivo que le proporcione una ubicación más exacta. Esto es un ejemplo de que, de forma predeterminada, sólo se envía información al servidor cuando es estrictamente necesario para procesar la solicitud del usuario. En cualquier caso, la información de la sesión se desecha después de 10 minutos de inactividad.

Cuando se utiliza Siri desde el Apple Watch, el reloj crea su propio identificador único aleatorio, como se describió anteriormente. Sin embargo, en lugar de volver a enviar la información del usuario, las solicitudes también envían el identificador de Siri del iPhone enlazado para proporcionar una referencia a dicha información.

La grabación de las palabras pronunciadas por el usuario se envía al servidor de reconocimiento de voz de Apple. Si la tarea sólo consiste en un dictado, el texto reconocido se envía de regreso al dispositivo. De lo contrario, Siri analiza el texto y, en caso necesario, lo combina con la información del perfil asociado al dispositivo. Por ejemplo, si la solicitud es "enviar un mensaje a mamá", se utilizan las relaciones y los nombres cargados desde Contactos. A continuación, el comando de la acción identificada se envía de vuelta al dispositivo para que se lleve a cabo.

El dispositivo realiza un gran número de funciones de Siri bajo la dirección del servidor. Por ejemplo, si el usuario le pide a Siri que lea un mensaje recién recibido, el servidor simplemente solicita al dispositivo que lea en voz alta el contenido de los mensajes no leídos. Ni los contenidos ni la información sobre el emisor se envían al servidor.

Las grabaciones de voz del usuario se guardan durante un periodo de seis meses, de modo que el sistema de reconocimiento las pueda utilizar para entender mejor la voz del usuario. Una vez transcurrido ese tiempo, se guarda otra copia sin el identificador correspondiente durante dos años como máximo para que Apple la use con el objetivo de mejorar y desarrollar Siri. Es posible que Apple siga usando por más de dos años un pequeño subconjunto de grabaciones, transcripciones y datos asociados sin identificadores para mejorar y asegurar la calidad de Siri. Además, algunas grabaciones que hacen referencia a música, equipos deportivos y deportistas, o empresas y puntos de interés se guardan de forma parecida con la finalidad de mejorar Siri.

También es posible utilizar Siri en modo manos libres mediante activación por voz. La detección de la activación por voz se realiza de forma local en el dispositivo. Así, Siri se activa únicamente cuando el patrón de audio de entrada coincide lo suficiente con la acústica de la frase de activación. Cuando se detecta la frase de activación, el audio correspondiente (incluido el comando posterior de Siri) se envía al servidor de reconocimiento de voz de Apple para continuar con su procesamiento, que sigue las mismas reglas que otras grabaciones de voz del usuario realizadas mediante Siri.

Continuidad

Continuidad saca provecho de tecnologías como iCloud, Bluetooth y Wi-Fi para permitir a los usuarios continuar con una actividad en otro dispositivo, hacer y recibir llamadas telefónicas, enviar y recibir mensajes de texto, y compartir la conexión a Internet de un dispositivo celular.

Handoff

Con Handoff, cuando la Mac y los dispositivos iOS de un usuario están cerca, el usuario puede transferir automáticamente aquello en lo que esté trabajando de un dispositivo al otro. Handoff permite al usuario cambiar de dispositivo y continuar trabajando de forma instantánea.

Cuando un usuario inicia sesión en iCloud en un segundo dispositivo compatible con Handoff, los dos dispositivos establecen un enlace mediante una conexión Bluetooth LE 4.0 fuera de banda a través del servicio APNs. Los mensajes individuales están encriptados de forma similar a como sucede en iMessage. Una vez que los dispositivos están enlazados, cada uno genera una clave simétrica AES de 256 bits que se almacena en el llavero del dispositivo. Esta clave puede encriptar y autenticar los avisos de la conexión Bluetooth LE que comunican la actividad actual del dispositivo con otros dispositivos enlazados de iCloud utilizando AES-256 en modo GCM con medidas de protección de reproducción. La primera vez que un dispositivo recibe un aviso de una clave nueva, establece una conexión Bluetooth LE con el dispositivo que origina la clave y genera un intercambio de claves de encriptación del aviso. Esta conexión se protege mediante la encriptación estándar Bluetooth LE 4.0 y la encriptación de los mensajes individuales, que es parecida a la encriptación de iMessage. En algunas situaciones, estos

mensajes se envían mediante APNs en lugar de mediante la conexión Bluetooth LE. La carga útil de la actividad se protege y se transfiere del mismo modo que con un iMessage.

Handoff entre apps nativas y sitios web

Handoff permite que una app nativa iOS pueda reanudar páginas web en dominios controlados legítimamente por el desarrollador de la app. También permite reanudar la actividad del usuario de la app nativa en un navegador web.

Con el fin de evitar que las apps nativas soliciten reanudaciones de sitios web no controlados por el desarrollador, las apps deben demostrar que disponen del control legítimo de los dominios web que desean reanudar. El control de un sitio web se establece a través del mecanismo para credenciales web compartidas. Para obtener más información, consulta el apartado "Acceso a contraseñas guardadas en Safari" en la sección "Encriptación y protección de datos" de este documento. El sistema debe validar el control del nombre del dominio de una app antes de que esta tenga permiso para aceptar la continuidad de la actividad del usuario con Handoff.

El origen de Handoff de una página web puede ser cualquier navegador que haya aceptado las API de Handoff. Cuando el usuario visualiza una página web, el sistema anuncia el nombre del dominio de la página web en los bytes de aviso de Handoff encriptados. Únicamente los demás dispositivos del usuario pueden desencriptar los bytes de aviso (como se describió anteriormente en esta sección).

En un dispositivo receptor, el sistema detecta que una app nativa instalada acepta Handoff desde el nombre de dominio anunciado y muestra el ícono de la app nativa como la opción de Handoff. Una vez abierta, la app nativa recibe la dirección URL completa y el título de la página web. No se transfiere ninguna otra información del navegador a la app nativa.

En el sentido inverso, una app nativa puede especificar una URL de respaldo cuando el dispositivo que recibe Handoff no tiene instalada la misma app nativa. En este caso, el sistema muestra el navegador predeterminado del usuario como opción de aplicación de Handoff (si ese navegador ha adoptado las API de Handoff). Cuando se solicite el uso de Handoff, el navegador se abrirá y se le facilitará la URL de respaldo que haya proporcionado la app nativa. No es necesario que la URL de respaldo se limite a los nombres de dominio que controle el desarrollador de la app nativa.

Handoff de datos de mayor tamaño

Como complemento a la función básica de Handoff, es posible que algunas apps elijan usar API que sean compatibles con el envío de un mayor número de datos mediante la tecnología de red Wi-Fi P2P creada por Apple (de forma parecida a AirDrop). Por ejemplo, la app Mail utiliza esas API para poder utilizar Handoff con borradores de mensajes de correo, que podrían incluir archivos adjuntos de gran tamaño.

Cuando una app utiliza esta función, el intercambio entre los dos dispositivos se inicia como en Handoff (véanse las secciones anteriores). Sin embargo, después de recibir la carga útil inicial mediante Bluetooth LE, el dispositivo receptor inicia una conexión nueva a través de la red Wi-Fi. Esta conexión está encriptada (TLS), con lo cual, intercambia sus certificados de identidad de iCloud. La identidad de los certificados se coteja con la identidad del usuario. El resto de los datos de carga útil se envía mediante esta conexión encriptada hasta que se completa la transferencia.

Portapapeles universal

El portapapeles universal aprovecha Handoff para transferir de forma segura el contenido del portapapeles del usuario a través de dispositivos para poder copiar contenido en un dispositivo y pegarlo en otro. El contenido se protege de la misma forma que los demás datos de Handoff y se comparte de forma predeterminada mediante el portapapeles universal, a menos que el desarrollador de la app decida desactivar la opción de compartir.

Las apps tienen acceso a los datos del portapapeles incluso si el usuario ha pegado el portapapeles en una app. Con el portapapeles universal, el acceso a estos datos se extiende a las apps que se están ejecutando en otros dispositivos del usuario (establecidos mediante sus sesiones abiertas de iCloud).

Desbloqueo automático

Las computadoras Mac compatibles con el desbloqueo automático usan Bluetooth LE y Wi-Fi P2P para permitir de forma segura que el Apple Watch del usuario desbloquee la Mac. Todas las Mac y Apple Watch compatibles que están asociados con una cuenta de iCloud deben usar la autorización de dos factores (TFA).

Cuando se permite que un Apple Watch desbloquee una Mac, se establece un enlace seguro mediante las identidades de desbloqueo automático. La Mac crea un secreto de desbloqueo aleatorio de un solo uso y lo transmite al Apple Watch mediante el enlace. El secreto se almacena en el Apple Watch y sólo se puede acceder a él cuando el Apple Wath esté desbloqueado (consulta la sección "Clases de protección de datos"). Ni la entropía principal ni el nuevo secreto son la contraseña del usuario.

Durante una operación de desbloqueo, la Mac utiliza Bluetooth LE para crear una conexión con el Apple Watch. A continuación, se establece un enlace seguro entre los dos dispositivos mediante las claves compartidas utilizadas cuando se activó por primera vez. Luego la Mac y el Apple Watch utilizan Wi-Fi P2P y una clave segura derivadas del enlace seguro para determinar la distancia entre los dos dispositivos. Si los dispositivos están dentro del alcance, el enlace seguro se utiliza para transferir el secreto previamente compartido para desbloquear la Mac. Después de desbloquearse, la Mac reemplaza el secreto de desbloqueo actual con un nuevo secreto de desbloqueo de uso único y transmite el nuevo secreto de desbloqueo al Apple Watch a través del enlace.

Retransmisión de llamadas telefónicas del iPhone

Cuando la Mac, iPad, o iPod touch de un usuario se encuentre en la misma red Wi-Fi que su iPhone, podrán realizar y recibir llamadas telefónicas utilizando la red celular del iPhone. La configuración requiere que los dispositivos hayan iniciado sesión tanto en iCloud como en FaceTime con la misma cuenta de Apple ID.

Al recibir una llamada entrante, todos los dispositivos configurados recibirán una notificación mediante el servicio de notificaciones push de Apple. Con cada notificación se usará la misma encriptación de punto a punto de iMessage. Los dispositivos que estén en la misma red presentarán la misma interfaz de notificación de llamada entrante. Después de responder la llamada, el audio se transmitirá sin interrupciones desde el iPhone del usuario utilizando una conexión P2P segura entre los dos dispositivos.

Cuando se responde una llamada en un dispositivo, se detiene el tono de llamada en los dispositivos enlazados con iCloud que estén cerca con un aviso mediante Bluetooth LE 4.0. Los bytes de aviso se encriptan usando el mismo método que los avisos de Handoff.

Las llamadas salientes también se transmiten al iPhone mediante el servicio de notificaciones push de Apple y el audio se transmite de forma parecida mediante el enlace P2P seguro entre dispositivos.

Los usuarios pueden desactivar la retransmisión de llamadas telefónicas en un dispositivo desactivando "Llamadas telefónicas del iPhone" en la configuración de FaceTime.

Reenvío de mensajes de texto del iPhone

La opción "Reenvío de mensajes de texto" permite enviar automáticamente los mensajes de texto SMS recibidos en un iPhone al iPad, iPod touch o Mac inscrito del usuario. Cada dispositivo debe haber iniciado sesión en el servicio iMessage con la misma cuenta de Apple ID. Cuando la función de reenvío de mensajes está activada, la inscripción de los dispositivos que están dentro del círculo de confianza del usuario —y que tienen la autenticación de dos factores activada— se realiza de forma automática. De lo contrario, el iPhone genera un código numérico de seis dígitos aleatorio que se ingresa en cada dispositivo para verificar su inscripción.

Una vez que los dispositivos están enlazados, el iPhone encripta y reenvía los mensajes de texto SMS entrantes a cada dispositivo mediante los métodos descritos en la sección iMessage de este documento. Las respuestas se envían de vuelta al iPhone utilizando el mismo método, y el iPhone las envía como mensajes de texto con ayuda del mecanismo de transmisión de SMS del operador. La opción para el reenvío de mensajes de texto se puede desactivar en la configuración de Mensajes.

Instant Hotspot

Los dispositivos iOS compatibles con Instant Hotspot usan la tecnología Bluetooth LE para descubrir y comunicarse con dispositivos que hayan iniciado sesión en la misma cuenta de iCloud. Las computadoras Mac compatibles que tienen el sistema operativo OS X Yosemite o posterior utilizan la misma tecnología para detectar dispositivos iOS y comunicarse con ellos mediante Instant Hotspot.

Cuando un usuario abre la configuración de Wi-Fi en un dispositivo iOS, este emite una señal Bluetooth LE que contiene un identificador común para todos los dispositivos que han iniciado sesión en la misma cuenta de iCloud. El identificador se genera desde un identificador DSID (Destination Signaling Identifier) vinculado a la cuenta de iCloud y va rotando periódicamente. Si hay otros dispositivos que hayan iniciado sesión en la misma cuenta de iCloud cerca y son compatibles con la función de compartir Internet, éstos detectarán la señal y responderán indicando su disponibilidad.

Cuando un usuario selecciona un dispositivo disponible para compartir Internet, se envía una solicitud de activación de "Compartir Internet" a dicho dispositivo. La solicitud se envía mediante un enlace que se encripta con la encriptación Bluetooth LE estándar, y la solicitud se encripta mediante un proceso parecido al de la encriptación de iMessage. A continuación, el dispositivo responde a través del mismo enlace de Bluetooth LE con la misma encriptación por mensaje con información de la conexión de "Compartir Internet".

Sugerencias de Safari, Sugerencias de Siri, Consultar, #images, app News, y widget de News en países sin News

Sugerencias de Safari, Sugerencias de Siri, Consultar, #images, la app News, y el widget de News en países sin News muestran a los usuarios sugerencias que van más allá de sus dispositivos, desde fuentes como Wikipedia, iTunes Store, noticias locales, resultados de Mapas y App Store; e incluso ofrece sugerencias antes de que el usuario comience a escribir.

Cuando un usuario comienza a escribir en la barra de direcciones de Safari, abre o usa Sugerencias de Siri, usa Consultar, abre #images, usa Buscar en la app News, o usa el widget de News en países sin News, se envía el siguiente contenido encriptado a Apple usando HTTPS con el fin de proporcionar resultados relevantes al usuario:

- Un identificador que cambia cada 15 minutos para mantener la privacidad.
- La consulta del usuario.
- La consulta completa más probable según el contexto y las búsquedas anteriores almacenadas en la caché.
- La ubicación aproximada del dispositivo, si "Localización" o "Sugerencias según ubicación" están activadas. El grado de aproximación de localización se basa en la densidad de población estimada en la ubicación del dispositivo; por ejemplo, en un entorno rural (donde los usuarios están más separados geográficamente) la aproximación usada es menor que en el caso del centro de una ciudad donde, normalmente, los usuarios estarán más cerca unos de otros. Los usuarios pueden desactivar el envío de toda la información de ubicación a Apple al desactivar Localización para las sugerencias según la ubicación desde Configuración. Si se desactiva Localización, Apple podría usar la dirección IP del dispositivo para calcular una ubicación aproximada.
- El tipo de dispositivo y si la búsqueda se realiza en Sugerencias de Siri en Buscar, Safari, Consultar, la app News o Mensajes.
- El tipo de conexión.
- La información de las tres apps usadas más recientemente en el dispositivo (para proporcionar contexto de búsqueda adicional). Sólo se incluyen apps que figuran en la lista blanca de Apple de apps populares y que se han accedido durante las últimas tres horas.
- Una lista de las aplicaciones populares del dispositivo.
- Preferencias de entrada, región e idioma.
- Si el dispositivo del usuario puede acceder a servicios de suscripción de música o video, se podría enviar a Apple información como los nombres de los servicios de suscripción y el tipo de suscripción. No se envía a Apple el nombre de la cuenta, el número y la contraseña del usuario.
- Representación resumida y sintetizada de los temas de interés

Cuando un usuario selecciona un resultado o sale de una app sin haber seleccionado un resultado, se envía a Apple cierta información para ayudar a mejorar la calidad de los resultados en el futuro. Esta información está vinculada sólo al identificador de sesión de 15 minutos y no a un usuario en particular. Esta retroalimentación incluye algunos elementos de la información de contexto descrita anteriormente, así como información de interacción como la siguiente:

- Intervalos de tiempo entre las interacciones y las solicitudes de la red de búsqueda.
- Clasificación y ordenado de las sugerencias.
- El ID del resultado y la acción seleccionados, si el resultado no es local, o la categoría del resultado seleccionado (si el resultado es local).
- Un indicador que indica si el usuario seleccionó el resultado.

Apple guarda registros de las sugerencias con las consultas, el contexto y la retroalimentación hasta por 18 meses. Además, se mantiene un subconjunto de registros hasta por cinco años (que incluye, por ejemplo, consultas, región, dominio, ubicación aproximada y estadísticas resumidas).

En algunos casos, las sugerencias pueden remitir las consultas sobre palabras y frases comunes a un socio calificado para recibir y mostrar los resultados de la búsqueda de dicho socio. Apple utiliza representaciones de las consultas de modo que los socios no reciben las direcciones IP o la retroalimentación de búsqueda de los usuarios. La comunicación con el socio se encripta mediante HTTPS. Para consultas frecuentes, Apple proporciona al socio la ubicación a nivel de ciudad, el tipo de dispositivo y el idioma del cliente como parte del contexto de búsqueda para mejorar el rendimiento de las búsquedas. En iOS 11, las consultas realizadas a través de las sugerencias de Siri en Buscar no se envían a los socios.

Para comprender y mejorar el rendimiento de las sugerencias de forma geográfica y a través de diferentes tipos de redes, se registra la siguiente información sin un identificador de sesión:

- Dirección IP parcial (sin el último octeto de las direcciones IPv4 o sin los últimos 80 bits de las direcciones IPv6)
- Ubicación aproximada
- Hora aproximada de la consulta
- Latencia/velocidad de transferencia
- Tamaño de la respuesta
- Tipo de conexión
- Región
- Tipo de dispositivo y app solicitante

Controles de dispositivos

iOS permite políticas de seguridad flexibles y configuraciones que son fáciles de aplicar y administrar. Gracias a estas políticas, las organizaciones pueden proteger su información corporativa y garantizar que sus empleados cumplan con los requisitos de la empresa, incluso si utilizan sus propios dispositivos, por ejemplo, como parte de un programa "traiga su propio dispositivo" (BYOD, por sus siglas en inglés).

Las organizaciones pueden utilizar recursos como la protección mediante código, los perfiles de configuración, el borrado remoto y las soluciones MDM de terceros para administrar conjuntos de dispositivos y ayudar a mantener la seguridad de los datos corporativos, incluso cuando los empleados accedan a dichos datos mediante sus propios dispositivos iOS.

Protección mediante código

De forma predeterminada, el código del usuario se puede definir como un PIN numérico. En dispositivos con Touch ID o Face ID, la extensión mínima del código es de seis dígitos. En otros dispositivos, la extensión mínima es de cuatro dígitos. Los usuarios pueden especificar un código alfanumérico de mayor longitud seleccionando "Código alfanumérico personalizado" en las "Opciones de código" de Configuración > Código. Se recomiendan los códigos más largos y más complejos, ya que son más difíciles de adivinar o atacar.

Los administradores pueden aplicar requisitos de uso de códigos complejos y otras políticas mediante MDM o Exchange ActiveSync, o bien pidiendo a los usuarios que instalen perfiles de configuración manualmente. Las siguientes políticas de código están disponibles:

- Permitir valor simple.
- Requerir valor alfanumérico.
- Longitud mínima del código.
- Número mínimo de caracteres complejos.
- Periodo máximo de validez del código.
- Historial de códigos.
- Tiempo de espera del bloqueo automático.
- Periodo de gracia para el bloqueo del dispositivo.
- Número máximo de intentos fallidos.
- Permitir Touch ID o Face ID.

Para consultar más información para administradores acerca de cada política, consulta: https://help.apple.com/deployment/ios/#/apd4D6A472A-A494-4DFD-B559-D59E63167E43.

Para consultar más información para desarrolladores acerca de cada política, consulta: https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/.

Modelo de enlace de iOS

iOS usa un modelo de enlace para controlar el acceso a un dispositivo desde una computadora host. El enlace establece una relación de confianza entre el dispositivo y el host conectado, representada mediante el intercambio de claves públicas. iOS utiliza esta señal de confianza para activar otras funcionalidades con el host conectado, como la sincronización de datos.

En iOS 9, los servicios que requieren enlace no pueden iniciarse hasta que el usuario haya desbloqueado el dispositivo.

Además, algunos servicios de iOS 10, como la sincronización de fotos, requieren que el dispositivo se desbloquee para que se puedan iniciar.

A partir de iOS 11, los servicios no se iniciarán a menos que el dispositivo se haya desbloqueado recientemente.

Para que el proceso de enlace se lleve a cabo, es necesario que el usuario desbloquee el dispositivo y acepte la solicitud de enlace del host. A partir de iOS 11, el usuario también deberá ingresar su código. Una vez hecho esto, el host y el dispositivo intercambian y guardan claves públicas RSA de 2048 bits. A continuación, el host recibe una clave de 256 bits con la que puede desbloquear un depósito de claves de custodia almacenado en el dispositivo (consulta "Custodia de depósitos de clave" en la sección "Depósitos de claves" de este documento). Las claves intercambiadas se utilizan para comenzar una sesión SSL encriptada, que el dispositivo necesita antes de enviar datos protegidos al host o de iniciar un servicio (sincronización con iTunes, transferencias de archivos, desarrollo con Xcode, etc.). El dispositivo requiere conexiones de un host mediante Wi-Fi para usar esta sesión encriptada para todas las comunicaciones, por ello es necesario que se haya enlazado previamente por USB. Además, el enlace también activa varias funciones de diagnóstico. En iOS 9, un registro de enlaces caduca si no se ha utilizado durante más de seis meses. Este periodo de tiempo se reduce a 30 días en iOS 11.

Para obtener más información, consulta:
https://support.apple.com/es-lamr/HT6331.

Ciertos servicios, como com.apple.pcapd, sólo pueden funcionar mediante USB. Además, el servicio com.apple.file_relay requiere la instalación de un perfil de configuración firmado por Apple.

En iOS 11, el Apple TV puede usar el protocolo de contraseña remota segura para establecer inalámbricamente una relación de enlazado.

El usuario puede borrar la lista de hosts de confianza con las opciones "Restablecer configuración de red" o "Restablecer localización y privacidad".

Para obtener más información, consulta:
https://support.apple.com/es-lamr/HT5868.

Aplicación de la configuración

Un perfil de configuración es un archivo XML que permite a un administrador distribuir información de configuración a dispositivos iOS. El usuario no puede modificar la configuración definida por un perfil de configuración instalado. Si el usuario elimina un perfil de configuración, también se eliminan todas las configuraciones establecidas por el perfil. De este modo, los administradores pueden aplicar configuraciones mediante la vinculación de las políticas al acceso a Wi-Fi y datos celulares. Por ejemplo, un perfil de configuración que proporciona una configuración de correo electrónico también puede especificar una política de códigos del dispositivo. Los usuarios no podrán acceder a los correos electrónicos a menos que su código cumpla con los requisitos del administrador.

Un perfil de configuración de iOS contiene una serie de configuraciones que se pueden especificar, incluidas las siguientes:

- Políticas de código.
- Restricciones en las funciones del dispositivo (por ejemplo, desactivar la cámara).
- Configuración de Wi-Fi.
- Configuración de VPN.
- Configuración del servidor de Mail.
- Configuración de Exchange.
- Configuración del servicio de directorio LDAP.
- Configuración del servicio de calendario CalDAV.
- Clips web.
- Credenciales y claves.
- Configuración avanzada de la red de telefonía celular.

Para ver una lista actual para administradores, consulta: https://help.apple.com/deployment/ios/#/cad5370d089.

Para ver una lista actual para los desarrolladores, consulta: https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/.

Los perfiles de configuración se pueden firmar y encriptar para validar su origen, garantizar su integridad y proteger su contenido. Los perfiles de configuración se encriptan usando CMS (RFC 3852) y son compatibles con 3DES y AES-128.

Además, se pueden bloquear en un dispositivo para evitar por completo su eliminación o para permitir su eliminación únicamente mediante un código. Dado que muchos usuarios empresariales son dueños de sus propios dispositivos iOS, se pueden eliminar los perfiles de configuración que vinculan un dispositivo con una solución MDM, pero a la vez se elimina toda la información de configuración administrada, los datos y las apps.

Los usuarios pueden instalar perfiles de configuración directamente en sus dispositivos utilizando Apple Configurator 2, o bien pueden descargarlos usando Safari, recibirlos mediante un mensaje de correo o descargarlos de forma inalámbrica usando una solución MDM. Cuando un usuario configura un dispositivo en el Programa de inscripción de dispositivos o Apple School Manager, el dispositivo descarga e instala un perfil de registro MDM.

Mobile Device Management (MDM)

Debido a que iOS es compatible con MDM, las empresas pueden configurar y administrar de manera segura las implementaciones graduales de Phone, iPad, Apple TV y Mac en sus organizaciones. Las funciones MDM están integradas en las tecnologías iOS actuales, tales como los perfiles de configuración, inscripción OTA y el servicio de notificaciones push de Apple. Por ejemplo, el APNs se utiliza para activar el dispositivo de manera que pueda comunicarse directamente con la solución MDM a través de una conexión segura. No se transmite información confidencial ni privada a través del APNs.

Con ayuda de MDM, los departamentos de TI pueden inscribir dispositivos iOS en un entorno empresarial, configurar los parámetros y actualizarlos mediante una red inalámbrica, supervisar el cumplimiento de políticas corporativas e incluso borrar o bloquear de forma remota los dispositivos administrados.

Para obtener más información sobre MDM, consulta: https://www.apple.com/la/business/resources/.

iPad compartido

"iPad compartido" es un modo multiusuario que se puede usar en las implementaciones educativas del iPad. Permite que los estudiantes compartan un iPad sin tener que compartir documentos y datos. Cada estudiante recibe su propio directorio de inicio, el cual se crea como un volumen APFS protegido por las credenciales del usuario. "iPad compartido" requiere el uso de un Apple ID administrado que sea propiedad y haya sido creado por la escuela. "iPad compartido" permite que un estudiante inicie sesión en cualquier dispositivo que sea propiedad de una organización y que esté configurado para que varios estudiantes lo usen.

Los datos de los estudiantes se dividen en particiones en directorios de inicio separados, cada uno en su propio dominio de protección de datos y protegido por permisos UNIX y aislamiento. Cuando un estudiante inicia sesión, el Apple ID administrado se autentica con los servidores de identidad de Apple usando el protocolo SRP. Si la autenticación se realiza correctamente, se concede un identificador de corta duración al dispositivo. Si el estudiante ha usado el dispositivo anteriormente, entonces ya existe una cuenta de usuario local que se puede desbloquear utilizando las mismas credenciales. Si el estudiante no ha usado el dispositivo antes, se le proporciona un ID de usuario UNIX, un volumen APFS con el directorio de inicio y un llavero lógico nuevos. Si el dispositivo no está conectado a Internet (por ejemplo, si está en un viaje escolar), la autenticación se puede llevar a cabo utilizando la cuenta local durante una cantidad limitada de días. En tal caso, sólo pueden iniciar sesión los usuarios que cuenten con una cuenta local. Una vez que caduca el tiempo límite, se requerirá que los estudiantes se autentifiquen en línea, incluso si ya existe una cuenta local.

Después de que la cuenta local del estudiante haya sido creada o desbloqueada, y si se autentica de forma remota, el identificador de corta duración concedido por los servidores de Apple se convierte en un identificador de iCloud que permite iniciar sesión en iCloud. Después, se restaura la configuración del estudiante y se sincronizan sus datos y documentos de iCloud.

Mientras la sesión del estudiante esté activa y el dispositivo permanezca en línea, los documentos y datos se almacenan en iCloud a medida que se creen o modifiquen. Además, un mecanismo de sincronización en segundo plano asegura que los cambios se envíen a iCloud después de que se cierre la sesión. Una vez que se completa la sincronización en segundo plano de ese usuario, se desmonta el volumen APFS del mismo y no se podrá volver a montar a menos que se ingresen las credenciales del usuario.

Cuando se actualiza un iPad compartido de una versión previa a iOS 10.3 a la versión 10.3 o posterior, se realiza una conversión única del sistema de archivos para convertir la partición de datos HFS+ a un volumen APFS. Si en ese momento hay directorios de inicio en el sistema, estos permanecerán en el volumen de datos principal en lugar de convertirse en volúmenes APFS individuales. Cuando más estudiantes inicien sesión, sus directorios de inicio también se colocarán en el volumen de datos principal. Las nuevas cuentas de usuario no se crearán con su propio volumen APFS, como se describió anteriormente, hasta que se hayan eliminado todas las cuentas de usuario del volumen de datos principal. Por lo tanto, para asegurarse de que los usuarios cuenten con las protecciones y cuotas adicionales que ofrece APFS, se debe actualizar el iPad a iOS 10.3 o posterior con la opción "Borrar y volver a instalar", o bien se deben eliminar todas las cuentas de usuario del dispositivo utilizando el comando MDM "Eliminar usuario".

Apple School Manager

Apple School Manager es un servicio para instituciones educativas que permite que compren contenido, configuren la inscripción automática de dispositivos en soluciones MDM, creen cuentas para estudiantes y personal, y configuren cursos de iTunes U. Apple School Manager se puede acceder desde la web y está diseñado para administradores de tecnología y de IT, personal y profesores.

Para obtener más información sobre Apple School Manager, consulta: https://help.apple.com/schoolmanager/.

Inscripción de dispositivos

El Programa de inscripción de dispositivos (DEP), parte de Apple School Manager y de los Programas de despliegue de Apple, proporciona una manera rápida y eficiente de desplegar dispositivo iOS que una organización haya adquirido directamente de Apple, o mediante distribuidores autorizados de Apple u operadores participantes. También es posible agregar dispositivos iOS con iOS 11 o posterior al DEP después de la fecha de compra mediante Apple Configurator 2.

Las organizaciones pueden inscribir automáticamente dispositivos en MDM sin tener que tocarlos físicamente ni prepararlos antes de que los usuarios los reciban. Después de inscribirse en el programa, los administradores inician sesión en el sitio web del programa y enlazan el programa con su solución MDM. A continuación, los dispositivos que hayan comprado se pueden asignar a los usuarios mediante el servidor MDM. Después de asignar el dispositivo a un usuario, todas las configuraciones, restricciones o controles específicos de MDM se instalan automáticamente. Todas las comunicaciones entre los dispositivos y los servidores de Apple se encriptan mediante HTTPS (SSL).

El proceso de configuración se puede simplificar todavía más para los usuarios al eliminar determinados pasos en el Asistente de Configuración, de modo que los usuarios puedan poner sus dispositivos en funcionamiento rápidamente. Los administradores también pueden controlar si el usuario puede o no borrar el perfil MDM desde el dispositivo y garantizar que las restricciones del dispositivo estén establecidas desde el principio. Una vez que se ha desempacado y activado el dispositivo, se puede inscribir en la solución MDM de la organización, de manera que se instalan todos los parámetros de administración, apps y libros.

Para obtener más información relacionada con las empresas, consulta: https://help.apple.com/deployment/business/.

Para obtener más información relacionada con las instituciones,consulta: https://help.apple.com/schoolmanager/.

Nota: la inscripción de dispositivos no está disponible en todos los países y regiones.

Apple Configurator 2

Además de MDM, Apple Configurator 2 para macOS facilita configurar y preconfigurar dispositivos iOS y Apple TV antes de dárselos a los usuarios. Apple Configurator 2 permite preconfigurar dispositivos rápidamente con apps, datos, restricciones y configuraciones.

Apple Configurator 2 te permite usar Apple School Manager (para educación) o el Programa de Inscripción de Dispositivos (para empresas) para registrar dispositivos en una solución MDM sin que los usuarios tengan que usar el asistente de configuración. Además, Apple Configurator 2 puede usarse para agregar dispositivos iOS y Apple TV al Apple School Manager o al Programa de inscripción de dispositivos después de la fecha de compra.

Para obtener más información sobre Apple Configurator 2, consulta: https://help.apple.com/configurator/mac/.

Supervisión

Durante la configuración de un dispositivo, una organización puede configurar la supervisión del dispositivo. La supervisión indica que el dispositivo es de propiedad institucional y proporciona un control adicional sobre su configuración y restricciones. Los dispositivos pueden supervisarse durante la configuración a través de Apple School Manager, el Programa de Inscripción de Dispositivos o de Apple Configurator 2. Para supervisar un dispositivo es necesario borrar y volver a instalar el sistema operativo.

Para obtener más información sobre la configuración y la administración de dispositivos con MDM o Apple Configurator 2, consulta: https://help.apple.com/deployment/ios/.

Restricciones

Los administradores pueden activar (o desactivar) restricciones para evitar que los usuarios accedan a apps, servicios o funciones específicas del dispositivo. Las restricciones se envían a los dispositivos en una carga útil de restricciones, la cual se adjunta a un perfil de configuración. Las restricciones se pueden aplicar a dispositivos con iOS, tvOS y macOS. Es posible que algunas restricciones aplicadas a un iPhone administrado se apliquen también a un Apple Watch enlazado.

Para ver una lista actual para los administradores de IT, consulta: https://help.apple.com/deployment/ios/#/apdbd6309354.

Borrado remoto

Los administradores o usuarios pueden borrar el contenido de los dispositivos iOS de forma remota. El borrado remoto instantáneo se consigue al descartar la clave de encriptación de almacenamiento de bloqueo de Effaceable Storage de forma segura, de modo que los datos ya no se pueden leer. Los comandos de borrado remoto se pueden inicializar desde MDM, Exchange o iCloud.

Cuando MDM o iCloud activan un comando de borrado remoto, el dispositivo envía una confirmación y realiza el borrado. En el caso del borrado remoto mediante Exchange, el dispositivo se registra en Exchange Server antes de realizar el borrado.

Los usuarios también pueden borrar el contenido de sus dispositivos mediante la app Configuración. Por último, como se ha mencionado anteriormente, los dispositivos se pueden configurar para que se realice un borrado automático del contenido después de una serie de intentos fallidos de ingresar el código.

Modo perdido

Si un dispositivo se pierde o lo roban, un administrador MDM puede activar de forma remota el modo perdido en un dispositivo supervisado que tenga iOS 9.3 o posterior. Cuando se activa el modo perdido, se cierra la sesión del usuario actual y el dispositivo no se puede desbloquear. La pantalla muestra un mensaje que el administrador puede personalizar, así que podría mostrar un número telefónico al que se puede llamar por si alguien encuentra el dispositivo. Cuando el dispositivo entra en el modo perdido, el administrador puede solicitar que el dispositivo envíe su ubicación actual y, opcionalmente, que reproduzca un sonido. Cuando el administrador desactiva el modo perdido (que es la única forma en la que se puede desactivar este modo), se le informa al usuario a través de un mensaje en la pantalla bloqueada o se muestra un aviso en la pantalla de inicio.

Bloqueo de activación

Cuando la función "Buscar mi iPhone" está activada, el dispositivo no se puede reactivar sin ingresar las credenciales del Apple ID del propietario o el código anterior del dispositivo.

En dispositivos que son propiedad de una organización, es buena idea supervisar los dispositivos para que la organización pueda administrar el bloqueo de activación en lugar de depender de un solo usuario para que ingrese sus credenciales de Apple ID para reactivar los dispositivos.

En dispositivos supervisados, una solución MDM compatible puede almacenar un código de anulación cuando el bloqueo de activación está activado o, después, usar este código para eliminar automáticamente el bloqueo si se tiene que borrar el contenido de un dispositivo para asignarlo a otro usuario.

De forma predeterminada, los dispositivos supervisados nunca tienen el bloqueo de activación activado, incluso aunque el usuario active "Buscar mi iPhone". Sin embargo, una solución MDM puede obtener un código de anulación y permitir que se active el bloqueo de activación en el dispositivo. Si "Buscar mi iPhone" está activada cuando la solución MDM habilita el bloqueo de activación, se activará en ese momento. Si "Buscar mi iPhone" está desactivada cuando el solución MDM habilita el bloqueo de activación, se activará la próxima vez que el usuario active "Buscar mi iPhone".

En dispositivos usados para la educación con un Apple ID administrado creado a través de Apple School Manager, el bloqueo de activación puede estar vinculado al Apple ID de un administrador en lugar del Apple ID del usuario; o también puede desactivarse usando el código de anulación del dispositivo.

Controles de privacidad

Apple se toma en serio la privacidad de los clientes y dispone de un gran número de controles integrados que permiten que los usuarios de iOS decidan cómo y cuándo las apps utilizan su información, así como qué información se utiliza.

Localización

Para determinar la ubicación aproximada del usuario, se utiliza información de GPS y Bluetooth, junto con los datos de antenas de telefonía celular y puntos activos de conexión Wi-Fi. La función Localización se puede desactivar fácilmente desde Configuración. Asimismo, los usuarios pueden aprobar el acceso de cada app que use este servicio. Puede que algunas apps soliciten recibir datos de ubicación sólo mientras la app esté en uso, o bien que soliciten recibirlos en cualquier momento. Si lo desean, los usuarios pueden rechazar este acceso o modificar su elección en cualquier momento desde Configuración. Desde Configuración, se puede elegir no permitir el acceso nunca, permitirlo únicamente mientras se use la app o permitirlo siempre, en función del uso que haga la app de la ubicación que solicite. Además, si las apps a las que se les ha concedido el permiso de uso de la ubicación en todo momento utilizan este permiso incluso en segundo plano, se recuerda a los usuarios que lo han aprobado y pueden realizar cambios en el acceso de la app.

De igual modo, a los usuarios se les otorga un control muy preciso sobre cómo los servicios del sistema utilizan datos relacionados a la ubicación. Esto incluye la posibilidad de desactivar la inclusión de información de ubicación en la información recopilada por los servicios de análisis utilizados por Apple para mejorar iOS, la información de Siri basada en la ubicación, el contexto basado en la ubicación para las búsquedas de las sugerencias de Siri, el estado del tráfico local y las ubicaciones importantes visitadas.

Acceso a datos personales

iOS evita que las apps puedan acceder sin permiso a la información personal del usuario. Además, en Configuración, los usuarios pueden ver cuáles son las apps a las que han otorgado acceso a determinada información, así como conceder o revocar permisos para cualquier acceso futuro. Esto incluye el acceso a:

- Contactos
- Calendarios
- Recordatorios
- Fotos
- Actividad y condición física
- Localización
- Apple Music
- Tu actividad de reproducción de música y videos
- Micrófono
- Cámara
- HomeKit
- Salud
- Reconocimiento de voz
- Compartir mediante Bluetooth
- Tu biblioteca de contenidos
- Cuentas de redes sociales tales como Twitter y Facebook

Si el usuario inicia sesión en iCloud, las apps tendrán permiso de acceso a iCloud Drive de forma predeterminada. Los usuarios pueden controlar el acceso de cada app a iCloud desde Configuración. Además, iOS proporciona restricciones que pueden impedir la transferencia de datos entre las apps y las cuentas que haya instalado una solución MDM y aquellas que haya instalado el usuario.

Política de privacidad

Para leer la política de privacidad de Apple, consulta: https://www.apple.com/la/legal/privacy/.

Recompensas de seguridad de Apple

Apple recompensa a los investigadores que comparten problemas graves con Apple. Para poder ser parte del programa de recompensas de seguridad de Apple, los investigadores deben proporcionar un reporte claro y pruebas de concepto válidas. La vulnerabilidad debe afectar la versión más reciente de iOS y, cuando aplique, el hardware más reciente. La cantidad de pago exacta será determinada por Apple después de su evaluación. Los criterios incluyen si se trata de un problema nuevo, la probabilidad de exposición y el grado de interacción del usuario.

Una vez que se hayan compartido adecuadamente los problemas, resolverlos lo más rápido posible se vuelve una prioridad para Apple. Cuando sea apropiado, Apple proporciona reconocimiento público a menos que se solicite lo contrario.

Categoría	Pago máximo (USD)
Componentes de firmware de arranque seguro	$200,000
Extracción de material confidencial protegido por Secure Enclave	$100,000
Ejecución de código arbitrario con privilegios del kernel	$50,000
Acceso no autorizado a los datos de la cuenta de iCloud en los servidores de Apple	$50,000
Acceso desde un proceso en una zona de seguridad a los datos de usuario que están fuera de esa zona de seguridad	$25,000

Conclusión

Compromiso con la seguridad

Apple se compromete a proteger a los clientes mediante destacadas tecnologías de privacidad y seguridad diseñadas para salvaguardar la información personal, así como mediante amplios métodos que ofrecen protección a los datos corporativos en entornos empresariales.

La seguridad está integrada en iOS. Desde la plataforma hasta las apps, pasando por las conexiones de red, todo lo que necesita una empresa está a su alcance en la plataforma iOS. La combinación de estos elementos permite a iOS contar con una seguridad líder en el sector sin que afecte la experiencia del usuario.

Apple utiliza una infraestructura de seguridad integrada y coherente en toda la plataforma iOS y en su ecosistema de apps. La encriptación de almacenamiento basada en el hardware ofrece la posibilidad de borrar el contenido de un dispositivo en caso de pérdida, y permite a los usuarios eliminar toda la información personal y corporativa si lo venden o lo transfieren a otro usuario. La información de diagnóstico también se recopila de manera anónima.

Las apps para iOS diseñadas por Apple se han creado teniendo en cuenta la mejora de la seguridad. Por ejemplo, iMessage y FaceTime proporcionan encriptación de cliente a cliente. En el caso de las apps de terceros, la combinación de la firma de código obligatoria, el aislamiento y las autorizaciones ofrecen a los usuarios una protección líder en la industria contra virus, software malicioso y otros ataques. La finalidad del proceso de entrega a la tienda App Store es seguir protegiendo a los usuarios de estos riesgos mediante la revisión de cada app para iOS antes de que se ofrezca.

Para aprovechar al máximo las amplias funciones de seguridad integradas en iOS, invitamos a que las empresas revisen sus políticas de TI y de seguridad para asegurarse de que se están beneficiando totalmente de las capas de tecnología de seguridad que ofrece esta plataforma.

Apple dispone de un equipo de seguridad experto con el fin de ofrecer soporte para todos sus productos. Este equipo realiza auditorías y pruebas de seguridad de los productos en proceso de desarrollo, así como de los productos que ya se lanzaron al mercado. Además, el equipo de Apple proporciona herramientas de seguridad y formación, y supervisa activamente si hay reportes de problemas y amenazas nuevas que pongan en riesgo la seguridad. Apple es miembro del Foro de equipos de seguridad y respuesta a incidentes (FIRST).

Para obtener más información sobre cómo reportar problemas a Apple y sobre la suscripción a las notificaciones de seguridad, consulta: https://www.apple.com/la/support/security.

Glosario

Actualización del firmware del dispositivo (DFU)	Modo en el que el código de la memoria ROM de arranque de un dispositivo espera su recuperación mediante USB. La pantalla está en negro; sin embargo, después de conectarse a una computadora en la que se ejecuta iTunes, se muestra el siguiente mensaje: "iTunes detectó un iPad en modo de recuperación. Es necesario restaurar el iPad para poder usarlo con iTunes."
Aleatorización del espacio de direcciones (ASLR)	Técnica que emplea iOS para que sea mucho más complicado conseguir aprovecharse de una vulnerabilidad de seguridad en el software. Al garantizar la impredecibilidad de las direcciones y los desplazamientos de la memoria, el código de ataque no puede incrustar esos valores en el código fuente. En iOS 5 o versiones posteriores, la ubicación de todas las apps y bibliotecas del sistema es aleatoria, igual que las apps de terceros compiladas como ejecutables con ubicación independiente.
Circuito integrado (IC)	También conocido como microchip.
Clave del sistema de archivos	Clave que encripta los metadatos de cada archivo, incluida la clave de clase correspondiente. Se guarda en la función Effaceable Storage para facilitar el borrado rápido, en lugar de la confidencialidad.
Clave por archivo	Clave AES de 256 bits que se usa para encriptar un archivo en el sistema de archivos. La clave por archivo se encapsula mediante una clave de clase y se almacena en los metadatos del archivo.
Correspondencia de ángulos del patrón de arrugas	Representación matemática de la dirección y el ancho de las arrugas extraída de una porción de una huella digital.
Depósito de claves	Estructura de datos que se utiliza para almacenar un conjunto de claves de clase. Cada tipo (usuario, dispositivo, sistema, respaldo, custodia o respaldo de iCloud) tiene el mismo formato: • Un encabezado que contiene: – La versión (configurada a 3 en iOS 5). – El tipo (sistema, respaldo, custodia o respaldo de iCloud). – El UUID del depósito de claves. – Un código HMAC si el depósito de claves está firmado. – El método usado para la encapsulación de las claves de clase: vinculado al UID o PBKDF2, junto con la sal y el conteo de iteraciones. • Una lista de claves de clase: – El UUID de las claves. – La clase (de qué clase de protección de datos de archivo o de llavero se trata). – El tipo de encapsulación (sólo clave derivada del UID; clave derivada del UID y clave derivada del código). – La clave de clase encapsulada. – La clave pública para clases asimétricas.
ECID	Identificador de 64 bits único en el procesador de cada dispositivo iOS. Cuando se responde una llamada en un dispositivo, se detiene el tono de llamada en los dispositivos enlazados con iCloud que estén cerca con un aviso mediante Bluetooth LE 4.0. Los bytes de aviso se encriptan usando el mismo método que los avisos de Handoff. Se usa como parte del proceso de personalización y no se considera un secreto.
Effaceable Storage	Área del almacenamiento NAND dedicada, utilizada para almacenar claves criptográficas, que se puede identificar directamente y borrar de forma segura. Aunque no ofrezca protección si un atacante dispone del dispositivo físicamente, las claves almacenadas en la función Effaceable Storage se pueden usar como parte de una jerarquía de claves para facilitar el borrado rápido y la consiguiente seguridad.

Encapsulación de claves	Encriptación de una clave con otra clave. iOS utiliza la encapsulación de claves AES del Instituto Nacional de Estándares y Tecnología (NIST), de acuerdo con la publicación RFC 3394.
Gestores de arranque de bajo nivel (LLB)	Código al que invoca la ROM de arranque y que, a su vez, carga iBoot como parte de la cadena de arranque seguro.
Grupo de acción de pruebas conjuntas (JTAG)	Herramienta estándar de depuración de hardware que usan programadores y desarrolladores de circuitos.
iBoot	Código que se carga mediante el LLB y que, a su vez, carga XNU como parte de la cadena de arranque seguro.
ID de grupo (GID)	Como el UID, pero común a todos los procesadores de una clase.
Identificador de recursos uniforme (URI)	Cadena de caracteres que identifica un recurso basado en web.
Identificador único (UID)	Clave AES de 256 bits que se graba en cada procesador durante el proceso de fabricación. Ni el firmware ni el software la pueden leer y solamente la usa el motor AES del hardware del procesador. Para obtener la clave real, un atacante tendría que crear un ataque físico muy sofisticado y caro contra el silicio del procesador. El UID no está relacionado con ningún otro identificador del dispositivo como, por ejemplo, el UDID.
Llavero	La infraestructura y un conjunto de API usadas por iOS y por apps de terceros para almacenar y recuperar contraseñas, claves y otras credenciales confidenciales.
Módulo de seguridad de hardware (HSM)	Computadora especializada en seguridad a prueba de manipulaciones que protege y administra claves digitales.
Perfil de datos	Archivo plist firmado por Apple que contiene una serie de entidades y autorizaciones que permiten instalar y probar apps en un dispositivo iOS. Un perfil de datos de desarrollo contiene una lista de dispositivos seleccionados por un desarrollador para realizar una distribución a medida, y un perfil de datos de distribución contiene el ID de app de una app desarrollada por una empresa.
Protección de datos	Mecanismo de protección de archivos y del llavero para iOS. También puede referirse a las API que utilizan las apps para proteger los archivos y los elementos del llavero.
ROM de arranque	El primer código que ejecuta el procesador de un dispositivo al encenderse por primera vez. Como parte integral del procesador, no lo pude alterar ni Apple ni ningún atacante.
Servicio de identidad (IDS)	Directorio de Apple de claves públicas de iMessage, direcciones del APNs, números de teléfono y direcciones de correo electrónico que se usan para buscar las claves y las direcciones de los dispositivos.
Servicio de notificaciones push de Apple (APNs)	Servicio ofrecido por Apple a nivel mundial que envía notificaciones push a los dispositivos iOS.
Sistema en un chip (SoC)	Circuito integrado (IC) que incorpora varios componentes en un único chip. El Secure Enclave es un SoC dentro de los procesadores centrales A7 o posteriores de Apple.
Tarjeta inteligente	Circuito integrado e incrustado que proporciona identificación, autenticación y almacenamiento de datos seguros.
Vinculación	Proceso mediante el cual el código de un usuario se convierte en una clave encriptada y se fortalece con el UID del dispositivo. Esto garantiza que un ataque de fuerza bruta se deba realizar en un dispositivo determinado y, por lo tanto, la velocidad esté limitada y el ataque no se pueda realizar en paralelo. El algoritmo de vinculación es PBKDF2, que usa AES encriptado con el UID del dispositivo como la función pseudoaleatoria (PRF) para cada iteración.
XNU	Kernel ubicado en el corazón de los sistemas operativos iOS y macOS. Se presupone que es de confianza, y refuerza las medidas de seguridad tales como la firma de código, el aislamiento, la comprobación de las autorizaciones y la ASLR.

Historial de revisión del documento

Fecha	Resumen
Enero de 2018	**Actualizado para iOS 11.2** • Apple Pay Cash **Actualizado para iOS 11.1** • Certificaciones de seguridad y programas • Touch ID/Face ID • Notas compartidas • Encriptación de punto a punto de CloudKit • TLS • Apple Pay y pagos con Apple Pay en la web • Sugerencias de Siri • iPad compartido • Para obtener más información sobre los contenidos de seguridad de iOS 11, consulta: https://support.apple.com/es-lamr/HT208112
Julio de 2017	**Actualizado para iOS 10.3** • System Enclave • Protección de datos de archivo • Depósitos de claves • Certificaciones de seguridad y programas • SiriKit • HealthKit • Seguridad de la red • Bluetooth • iPad compartido • Modo perdido • Bloqueo de activación • Controles de privacidad • Para obtener más información sobre los contenidos de seguridad de iOS 10.3, consulta: http://support.apple.com/es-lamr/HT207617
Marzo de 2017	**Actualizado para iOS 10** • Seguridad del sistema • Clases de protección de datos • Certificaciones de seguridad y programas • HomeKit, ReplayKit y SiriKit • Apple Watch • Wi-Fi, VPN • Inicio de sesión único (SSO) • Apple Pay y pagos con Apple Pay en la web • Datos de tarjetas de crédito, débito y prepago • Sugerencias de Safari • Para obtener más información sobre los contenidos de seguridad de iOS 10, consulta: http://support.apple.com/es-lamr/HT207143

Fecha	Resumen
Mayo de 2016	**Actualizado para iOS 9.3** • Apple ID administrado • Autenticación de dos factores para Apple ID • Depósitos de claves • Certificaciones de seguridad • Modo perdido y bloqueo de activación • Notas seguras • Apple School Manager y iPad compartido • Para obtener más información sobre los contenidos de seguridad de iOS 9.3, consulta: https://support.apple.com/es-lamr/HT206166
Septiembre de 2015	**Actualizado para iOS 9** • Bloqueo de activación de Apple Watch • Políticas de código • Compatibilidad API de Touch ID • Protección de datos en A8 mediante AES-XTS • Depósitos de claves para la actualización de software sin supervisión • Actualización de certificados • Modelo de confianza de apps empresariales • Protección de datos para los marcadores de Safari • Seguridad de transporte de las apps • Especificaciones de VPN • Acceso remoto a iCloud para HomeKit • Tarjetas de recompensa de Apple Pay y app de la entidad emisora de la tarjeta de Apple Pay • Indexación de Spotlight en el dispositivo • Modelo de enlace de iOS • Apple Configurator 2 • Restricciones • Para obtener más información sobre los contenidos de seguridad de iOS 9, consulta: https://support.apple.com/es-lamr/HT205212

Enero de 2018