



Seguridad de iOS

Octubre de 2014
iOS 8.1 o posterior

Contenido

Página 4 Introducción

Página 6 Seguridad del sistema

- Cadena de arranque seguro
- Autorización del software del sistema
- Secure Enclave
- Touch ID

Página 11 Encriptación y protección de datos

- Funciones de seguridad de hardware
- Protección de datos de archivo
- Códigos
- Clases de protección de datos
- Protección de datos de llavero
- Acceso a contraseñas guardadas en Safari
- Repositorios de claves
- FIPS 140-2

Página 20 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
- HealthKit

Página 28 Seguridad de la red

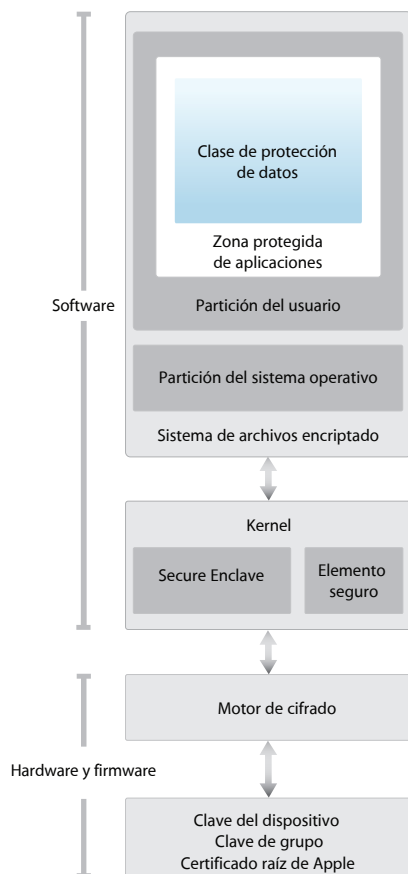
- SSL y TLS
- VPN
- Wi-Fi
- Bluetooth
- Inicio de sesión único
- Seguridad de AirDrop

Página 32 Servicios de Internet

- ID de Apple
- iMessage
- FaceTime
- iCloud
- Llavero de iCloud
- Siri
- Continuity
- Sugerencias de Spotlight

Página 46	Controles del dispositivo
	Protección mediante código
	Modelo de enlace de iOS
	Ejecución de la configuración
	Mobile Device Management (MDM)
	Programa de inscripción de dispositivos
	Apple Configurator
	Restricciones del dispositivo
	Restricciones solo supervisadas
	Borrado remoto
	Buscar mi iPhone y Bloqueo de activación
Página 53	Controles de privacidad
	Localización
	Acceso a datos personales
	Política de privacidad
Página 55	Conclusión
	Compromiso con la seguridad
Página 56	Glosario

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 de escritorio y definimos un enfoque nuevo de la 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 conjuntamente con el fin de proporcionar la máxima seguridad y una experiencia de usuario transparente. iOS protege el dispositivo y los datos que 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.

iOS y los dispositivos iOS proporcionan funciones de seguridad avanzadas y, además, son fáciles de usar. Muchas de estas funciones están activadas por omisión, por lo que los departamentos de TI no tienen que llevar a cabo demasiadas configuraciones. Además las funciones de seguridad clave, como la encriptación de los dispositivos, no se pueden configurar, de este modo, se evita que los usuarios las desactiven por error. Otras funciones, como Touch 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 será de ayuda a las organizaciones que quieran combinar la tecnología y las funciones de seguridad de la plataforma iOS con sus propias políticas y procedimientos a fin de satisfacer sus necesidades de seguridad específicas.

Este documento se divide en los temas siguientes:

- **Seguridad del sistema:** el software y el 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.
- **Servicios de Internet:** la infraestructura basada en red de Apple para los servicios de mensajería, sincronización y copia de seguridad.

- **Controles de dispositivos:** los métodos que impiden el uso no autorizado del dispositivo y hacen posible borrar su contenido remotamente en caso de pérdida o robo.
- **Controles de privacidad:** las prestaciones de iOS que se pueden utilizar para controlar el acceso a la función de localización y a los datos de usuario.

Seguridad del sistema

Acceso 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 solo hay código firmado por Apple no modificado. Se puede entrar en modo DFU manualmente: en primer lugar, conecte el dispositivo a un ordenador mediante un cable USB y, a continuación, mantenga pulsados los botones de inicio y de activación/reposo. Tras 8 segundos suelte el botón de activación/reposo y siga manteniendo pulsado el botón de inicio.

Nota: no se mostrará ninguna información en la pantalla mientras el dispositivo esté en modo DFU. Si aparece el logotipo de Apple, habrá pulsado durante demasiado tiempo el botón de activación/reposo.

La seguridad del sistema se ha diseñado de modo que tanto el software como el hardware estén 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 de iOS y en ningún caso interfiere en la utilización del dispositivo.

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

Cadena de arranque seguro

Todos los pasos del proceso de arranque contienen componentes firmados mediante cifrado por Apple para garantizar su integridad y el avance únicamente después de haber verificado la cadena de confianza. Esto incluye los cargadores de arranque, el kernel, las extensiones del kernel y el firmware de banda base.

Cuando se enciende un dispositivo iOS, el procesador de aplicaciones ejecuta inmediatamente código de la memoria de solo lectura (o ROM de arranque). Este código inmutable, que también se conoce como raíz de confianza de hardware, se establece durante la fabricación del chip y es de confianza implícitamente. El código de la ROM de arranque contiene la clave pública de la entidad emisora de certificados (CA) raíz de Apple, que se utiliza para verificar que el cargador de arranque de bajo nivel (LLB) tiene la firma de Apple antes de permitir que se cargue. Este es el primer paso de la cadena de confianza, en la que cada paso garantiza que el siguiente está firmado por Apple. Cuando el LLB termina sus tareas, verifica y ejecuta el cargador de arranque de la siguiente fase (iBoot), que a su vez verifica y ejecuta el kernel de iOS.

La cadena de arranque seguro ayuda a garantizar que no se han manipulado los niveles de software inferiores y permite que iOS se ejecute únicamente en dispositivos Apple validados.

En el caso de los dispositivos que disponen de acceso a datos móviles, 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 tienen un procesador A7 o uno posterior de la serie A, 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.

Si un paso de este proceso de arranque no consigue cargar o verificar el siguiente proceso, se detiene el arranque y el dispositivo muestra la pantalla “Conectarse a iTunes”. Es lo que se conoce como modo de recuperación. Si la ROM de arranque no consigue cargar o verificar el LLB, entra en modo de actualización del firmware del dispositivo (DFU). En ambos casos, el dispositivo debe conectarse a iTunes mediante USB y se deben restaurar los ajustes originales de fábrica. Para obtener más información acerca de cómo acceder manualmente al modo de recuperación, consulte el artículo https://support.apple.com/kb/HT1808?viewlocale=es_ES.

Autorización del software del sistema

Apple publica periódicamente actualizaciones de software que abordan los nuevos riesgos de seguridad y ofrecen nuevas funciones. Estas actualizaciones se proporcionan, de forma 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 por vía inalámbrica, para así facilitar la instalación de las correcciones de seguridad más recientes.

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

En los dispositivos con un procesador A7 o uno posterior de la serie A, el coprocesador Secure Enclave también utiliza el proceso de autorización del software del sistema para garantizar la integridad de su software y evitar la instalación de versiones anteriores. Consulte la sección “Secure Enclave” más abajo.

Las actualizaciones de software iOS se pueden instalar a través de iTunes o de forma remota (OTA) en el dispositivo. Con iTunes, se descarga e instala una copia completa de iOS. Las actualizaciones de software OTA solo 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. Además, las actualizaciones de software se pueden almacenar en caché en un servidor de red local que ejecute el servicio de almacenamiento en memoria caché en OS X Server, de manera que los dispositivos iOS no tengan que acceder a los servidores de Apple para obtener los datos de actualización necesarios.

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 de cifrado para cada parte del paquete de instalación que se vaya a instalar (por ejemplo, el LLB, iBoot, el kernel o una imagen del sistema operativo), un valor antirreproducción aleatorio (nonce) 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, añade 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. La adición del ECID “personaliza” la autorización para el dispositivo que realiza la solicitud. El servidor solo 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 durante el arranque, se verifica que la firma procede de Apple y que la medida del ítem cargado desde el disco —combinada con el ECID del dispositivo— coincide con el contenido de lo firmado.

Estos pasos garantizan que la autorización es para un dispositivo específico e impiden que una versión de iOS antigua se copie de un dispositivo a otro. El nonce 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 el procesador A7 o uno posterior de la serie A de Apple. Este coprocesador utiliza un arranque seguro y una actualización de software personalizada diferentes a los que utiliza el procesador de aplicaciones. Proporciona todas las operaciones cifradas para la gestión de claves de protección de datos y mantiene la integridad de la protección de datos aunque la seguridad del kernel esté en peligro.

El Secure Enclave utiliza memoria encriptada e incluye un generador de números de hardware aleatorios. Su microkernel se basa en la familia L4, con alguna modificación por parte de Apple. La comunicación entre el Secure Enclave y el procesador de aplicaciones se aísla en un buzón basado en interrupciones y en búferes de datos de memoria compartida.

Durante el proceso de fabricación, se proporciona a cada Secure Enclave un identificador único (UID) propio que Apple no conoce y al que otras partes del sistema no tienen acceso. Cuando el dispositivo se enciende, se crea una clave efímera —vinculada a su UID—, que se utiliza para encriptar la parte que ocupa el Secure Enclave en el espacio de la memoria del dispositivo.

Además, los datos que el Secure Enclave guarda en el sistema de archivos se encriptan con una clave vinculada al UID y un contador antirreproducciones.

El coprocesador Secure Enclave es el responsable de procesar los datos de huella digital del sensor Touch ID y determinar si coinciden con alguna de las huellas registradas, en cuyo caso permitirá el acceso o las compras en nombre del usuario. La comunicación entre el procesador y el sensor Touch ID tiene lugar a través de un bus de interfaz de periféricos serie. El procesador envía los datos al Secure Enclave, pero no puede leerlos, puesto que están encriptados y se autentican mediante una clave de sesión que se negocia con la clave compartida del dispositivo proporcionada para el sensor Touch ID y el Secure Enclave. 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.

Touch ID

Touch ID es el sistema de detección de huellas digitales que hace posible un acceso seguro, más rápido y sencillo al dispositivo. 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 en cada uso al identificar nuevos nodos superpuestos.

Gracias a Touch ID, los usuarios no tienen que introducir el código muy a menudo, por lo que pueden utilizar uno más largo y complejo. Además Touch ID evita la incomodidad del bloqueo basado en código al proporcionar acceso seguro al dispositivo en poco tiempo y con restricciones específicas, aunque no lo reemplaza.

Touch ID y códigos

Para utilizar Touch ID, los usuarios deben configurar su dispositivo, de modo que se requiera un código para desbloquearlo. Cuando Touch ID escanea y reconoce una huella digital registrada, el dispositivo se desbloquea sin solicitar el código. El código se puede utilizar en vez de Touch ID en cualquier circunstancia, 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 el dispositivo ha recibido un comando de bloqueo remoto.
- Cuando, tras cinco intentos, no se ha reconocido una huella digital.
- Cuando se configura Touch ID o se registran nuevas huellas digitales.

Si Touch ID está activado, el dispositivo se bloquea de inmediato al pulsar el botón de activación/reposo. Muchos de los usuarios que solo utilizan el código como sistema de seguridad establecen un periodo de gracia de desbloqueo para no tener que introducir el código cada vez que quieran utilizar el dispositivo. Si se utiliza Touch ID, el dispositivo se bloquea cada vez que entra en reposo y siempre se requiere la huella (o el código) para activarlo.

Touch ID se puede configurar para que reconozca un máximo de cinco huellas digitales. Si solo se registra una huella, la posibilidad de una coincidencia aleatoria con otra persona es de 1 entre 50.000. No obstante, Touch ID solo permite cinco intentos fallidos de acceder con huella digital y después será necesario introducir el código para obtener acceso.

Otros usos de Touch ID

Touch ID también se puede configurar para aprobar compras en las tiendas iTunes Store, App Store y iBooks Store, de modo que los usuarios no tienen que introducir la contraseña de su ID de Apple. Cuando un usuario autoriza una compra, el dispositivo y la tienda intercambian identificadores de autenticación. El identificador y el nonce cifrado se guardan en el coprocesador Secure Enclave. El nonce se firma con una clave del Secure Enclave que comparten todos los dispositivos y la tienda iTunes Store.

Además, las apps de terceros pueden utilizar las API proporcionadas por el sistema para solicitar al usuario que se autentique con Touch ID o un código. Solo se informa a la app de si la autenticación se ha realizado correctamente o no, pero no se le proporciona acceso ni a Touch ID ni a los datos asociados con la huella digital registrada.

Los ítems del llavero también se pueden proteger con Touch ID, de modo que el Secure Enclave solo los desbloquee con una huella coincidente o con el código del dispositivo. Los desarrolladores de apps también disponen de API para verificar si el usuario ha establecido un código y, por lo tanto, es posible autenticar o desbloquear ítems del llavero con Touch ID.

Seguridad de Touch ID

El sensor de huellas digitales solo está activado cuando el anillo de acero capacitivo que rodea al 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 imagen escaneada —de 88 x 88 píxeles y 500 ppp— 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 ángulos del patrón de arrugas subdérmico; este proceso propenso a la pérdida de información 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 solo el Secure Enclave puede leer, y nunca se envía a Apple ni se copia en iCloud o iTunes.

Cómo Touch ID desbloquea un dispositivo iOS

Si Touch ID está desactivado, cuando se bloquea un dispositivo, se descartan las claves de la clase de protección de datos “Complete”, que se almacenan en el Secure Enclave. No se podrá acceder a los archivos e ítems del llavero de dicha clase hasta que el usuario desbloquee el dispositivo con su código.

Si Touch ID está activado, 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 en el Secure Enclave. Cuando un usuario intenta desbloquear el dispositivo, Touch ID proporciona (si reconoce la huella del usuario) la clave para desencapsular las claves de protección de datos, y el dispositivo se desbloquea. Este proceso ofrece protección adicional al requerir a los subsistemas de Touch ID y de protección de datos que colaboren para desbloquear el dispositivo.

Las claves que Touch ID necesita para desbloquear el dispositivo se pierden al reiniciar el dispositivo y el Secure Enclave las descarta a las 48 horas o tras cinco intentos de reconocimiento fallidos de Touch ID.

Encriptación y protección de datos

La cadena de arranque seguro, la firma de código y la seguridad del proceso de ejecución garantizan que, en un dispositivo, solo se puedan ejecutar apps y código que sean de confianza. iOS dispone de otras funciones de encriptación y de protección de datos para proteger los datos del usuario, incluso cuando otras partes de la infraestructura de seguridad están 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 móviles, la velocidad y la eficiencia energética son factores fundamentales. Las operaciones cifradas son complejas y pueden provocar problemas de rendimiento o 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 cifrado 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.

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 solo 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, solo el motor AES dedicado al Secure Enclave puede utilizar estos UID y GID del Secure Enclave. Los UID son exclusivos de cada dispositivo y no los registra ni Apple ni ninguno de sus proveedores. Los GID son comunes a todos los procesadores de una clase de dispositivos (por ejemplo, todos los dispositivos que utilizan el procesador A8 de Apple) y se utilizan para tareas que no son fundamentales para la seguridad, como la distribución del software del sistema durante los procesos de instalación y restauración. La integración de estas claves en el silicio ayuda a prevenir su manipulación o desactivación, así como el acceso a ellas fuera del motor AES. El UID y el GID tampoco están disponibles a través de JTAG u otras interfaces de depuración.

El UID permite vincular los datos a un dispositivo determinado mediante cifrado. 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.

Salvo el UID y el GID, todas las claves cifradas 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 gestión de las interrupciones

Borrar contenidos y ajustes

Esta opción de Ajustes borra todas las claves de la función Effaceable Storage, de manera que se deja de poder acceder a todos los datos del usuario en el dispositivo mediante cifrado. 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 utilice la opción "Borrar contenidos y ajustes" hasta que se haya realizado una copia de seguridad del dispositivo, ya que los datos eliminados no se podrán recuperar.

tras el encendido. Las claves generadas en el Secure Enclave utilizan su generador de números aleatorios de hardware 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, 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 abordar directamente y borrar un número reducido de bloques a un nivel muy bajo.

Protección de datos de archivo

Además de las funciones de encriptación de 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 permite que el dispositivo responda ante eventos habituales, como las llamadas de teléfono entrantes, pero 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 por omisión, y las apps de terceros instaladas en iOS 7 o posterior reciben esta protección de forma automática.

La protección de datos se implementa mediante la creación y gestión 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 en función de si las claves de clase se han desbloqueado o no.

Visión general de la arquitectura

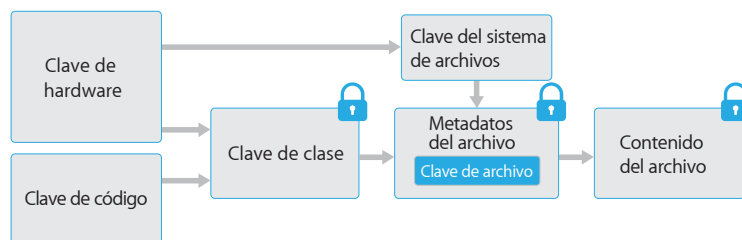
Cada vez que se crea un archivo en la partición de datos, la función de protección de datos crea una nueva clave de 256 bits (la clave “por archivo”) y se la proporciona al motor AES de hardware, que utiliza la clave para encriptar el archivo como si se hubiese escrito en la memoria flash con el modo CBC de AES. 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 se empaqueta 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.

Al abrir un archivo, sus metadatos se desencriptan con la clave del sistema de archivos y, entonces, se muestra la clave por archivo encapsulada y una notación sobre la clase que lo protege. La clave por archivo 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.

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. La clave del sistema de archivos se almacena en Effaceable Storage. Como se almacena en el dispositivo, esta clave no se utiliza para preservar la confidencialidad de los datos, sino que se ha diseñado para permitir su borrado rápido por petición (los usuarios pueden hacerlo con la opción “Borrar contenidos y ajustes”, y los administradores o usuarios, mediante un comando de borrado remoto desde

un servidor Mobile Device Management [MDM], desde Exchange ActiveSync o desde iCloud). Al borrar la clave de esta manera, se deja de poder acceder a todos los archivos mediante cifrado.



El contenido de un archivo se encripta con una clave por archivo, que se encapsula con una clave de clase y se almacena en los metadatos del archivo, que a su vez se encripta 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 y un cambio del código volverá a encapsular la clave de clase.

Códigos

Al configurar un código de dispositivo, el usuario activa la protección de datos automáticamente. iOS admite códigos alfanuméricos de 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 se haya hecho con 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 tendrá 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.

Cuanto más seguro sea el código del usuario, más segura será la clave de encriptación. Touch ID se puede utilizar 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.

A fin de desalentar aún más los posibles ataques de fuerza bruta, la interfaz de iOS aplica tiempos de demora cada vez mayores tras la introducción de un código no válido en la pantalla de bloqueo. Si lo desean, los usuarios pueden configurar el dispositivo para que su contenido se borre automáticamente tras 10 intentos fallidos de introducir el código correcto. Este ajuste, 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 procesador A7 o posterior de la serie A, el Secure Enclave se ocupa de las operaciones de claves y aplica una demora de 5 segundos entre cada nueva solicitud de desbloqueo fallida. El objetivo es proporcionar un regulador frente a ataques de fuerza bruta, además de las medidas de protección de iOS.

Consideraciones sobre la contraseña

Si se introduce 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 introducir un código numérico largo que un código alfanumérico corto, aunque ambos proporcionen un nivel de seguridad parecido.

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.

Complete Protection

(`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 bloquee un dispositivo (10 segundos, si el ajuste de “Solicitar contraseña” es “De inmediato”), se descarta la clave de clase descriptada, de modo que se deja de poder acceder a todos los datos de esta clase hasta que el usuario vuelva a introducir el código o desbloquee el dispositivo con Touch ID.

Protected Unless Open

(`NSFileProtectionCompleteUnlessOpen`): Es posible que sea necesario escribir en algunos archivos mientras el dispositivo está bloqueado. Por ejemplo, al descargar un archivo adjunto de correo en segundo plano. Este comportamiento se consigue con la criptografía de curva elíptica asimétrica (ECDH sobre Curve25519). Las claves por archivo normales están protegidas con una clave obtenida según el acuerdo de claves de Diffie-Hellman de un paso, tal como se describe en la publicación SP 800-56A del NIST.

La clave pública efímera del acuerdo se almacena junto la clave por archivo encapsulada. KDF es el acrónimo de “Concatenation Key Derivation Function” (función de derivación de claves de concatenación) (Alternativa aprobada 1), tal como se describe en la sección 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; y 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 con clave privada de la clase Protected Unless Open y la clave pública efímera del archivo; el hash se utiliza para desencapsular la clave por archivo, que después se utiliza para descriptar el archivo.

Protected Until First User Authentication

(`NSFileProtectionCompleteUntilFirstUserAuthentication`): Esta clase se comporta del mismo modo que Complete Protection, con la diferencia de que la clave de clase descriptada 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 por omisión para todos los datos de apps de terceros que no tengan una clase de protección de datos asignada por otra vía.

No Protection

(`NSFileProtectionNone`): Esta clave de clase solo está protegida con el UID y se guarda en Effaceable Storage. Dado que todas las claves necesarias para descriptar los archivos de esta clase se almacenan en el dispositivo, la encriptación solo añade 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).

Componentes de un ítem del llavero

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

También contienen los hash SHA-1 de los atributos usados para la consulta del ítem (tales como el nombre de cuenta y de servidor) para permitir que se realicen búsquedas sin desencriptar cada ítem. 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 ítem;
- clave por ítem encapsulada con la clave de clase de protección;
- diccionario de atributos que describen el ítem (tras transferirse a `SecItemAdd`), codificado como un archivo plist binario y encriptado con la clave por ítem.

La encriptación es AES 128 en modo de contador Galois (GCM); el grupo de acceso se incluye en los atributos y se protege mediante la etiqueta GMAC que se calcula durante la encriptación.

Protección de datos de llavero

Muchas apps necesitan gestionar 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 ítems.

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

Los ítems del llavero solo se pueden compartir entre las apps de un mismo desarrollador. Esto se gestiona solicitando a las apps de terceros que utilicen grupos de acceso con un prefijo asignado a través del programa para desarrolladores de iOS o, en iOS 8, 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 iOS.

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 API con nombres diferentes.

Disponibilidad	Protección de datos de archivo	Protección de datos de llavero
Cuando está desbloqueado	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
Cuando está bloqueado	NSFileProtectionCompleteUnlessOpen	N/A
Tras el 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 ítems del llavero a los que es necesario acceder durante este tipo de actualizaciones.

La clase `kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly` solo está disponible cuando el dispositivo tiene un código configurado. Los ítems de esta clase solo existen en el repositorio de claves del sistema; no se sincronizan con el llavero de iCloud, no se incluyen en repositorios de claves de custodia ni se hacen copias de seguridad de ellos. Si se elimina o restablece el código, se descartan las claves de clase y los ítems dejan de ser útiles.

Otras clases de llavero tienen un equivalente a “This device only”, que siempre está bajo la protección del UID cuando se copia del dispositivo durante la copia de seguridad, de modo que deja de ser útil si se restaura en un dispositivo diferente.

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 ítems de llavero creados por iOS, se aplican las siguientes protecciones de clase:

Ítem	Accesible
Contraseñas Wi-Fi	Tras el primer desbloqueo
Cuentas de Mail	Tras el primer desbloqueo
Cuentas de Exchange	Tras el primer desbloqueo
Contraseñas VPN	Tras el primer desbloqueo
LDAP, CalDAV y CardDAV	Tras el primer desbloqueo
Identificadores de cuentas de redes sociales	Tras el primer desbloqueo
Claves de encriptación de anuncios de Handoff	Tras el primer desbloqueo
Identificador de iCloud	Tras el primer desbloqueo
Contraseña de “Compartir en casa”	Cuando está desbloqueado
Identificador de Buscar mi iPhone	Siempre
Buzón de voz	Siempre
Copia de seguridad de iTunes	Cuando está desbloqueado, no migratorio
Contraseñas 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 el 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 ítems 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 o que se introduzca el código del dispositivo. Las ACL se evalúan en el Secure Enclave y solo se desbloquean en el kernel si se cumplen las restricciones especificadas.

Acceso a contraseñas guardadas en Safari

Las apps iOS pueden interactuar con ítems del llavero guardados en Safari para el autorrelleno de contraseñas con las dos API siguientes:

- `SecRequestSharedWebCredential`
- `SecAddSharedWebCredential`

Solo 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 firmado en CMS en su servidor donde se indiquen los identificadores de apps exclusivos de las apps que hayan aprobado. Cuando se instala una app con la autorización `com.apple.developer.associated-domains`, iOS 8 envía una solicitud de TLS a cada sitio web de la lista para solicitar el archivo `/apple-app-site-association`. Si la firma procede de una identidad válida para el dominio y es de confianza para iOS, y el archivo incluye en su lista el identificador de la app que se está instalando, iOS marca la relación del sitio web y la app como de confianza. Las llamadas a estas dos API solo generan una solicitud para el usuario cuando existe una relación de confianza; para que se lleve a cabo la entrega de contraseñas a la app o para que se actualicen o eliminen, es necesaria la aceptación del usuario.

Repositorios de claves

Las claves para las clases de protección de datos de llavero y de archivo se recopilan y gestionan en repositorios de claves. iOS utiliza los cuatro siguientes: repositorio de claves del sistema, de copia de seguridad, de custodia y de copia de seguridad de iCloud.

El repositorio de claves del sistema, 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 introduce un código, se carga la clave `NSFileProtectionComplete` del repositorio de claves del sistema y se desencapsula. Se trata de un archivo plist binario almacenado en la clase `No Protection`, pero cuyo contenido está encriptado con una clave que se guarda en `Effaceable Storage`. A fin de proporcionar mayor seguridad a los repositorios de claves, esta clave se borra y se vuelve a generar cada vez que un usuario cambia el código. La extensión del kernel `AppleKeyStore` gestiona el repositorio de claves del sistema y admite consultas relativas al estado de bloqueo del dispositivo. Solo indica que el dispositivo está desbloqueado si se puede acceder a todas las claves de clase del repositorio de claves del sistema y si se han desencapsulado correctamente.

El repositorio de claves de copia de seguridad se crea cuando iTunes realiza una copia de seguridad encriptada y la almacena en el ordenador donde se efectúa la copia de seguridad del dispositivo. Se crea un repositorio de claves nuevo con un conjunto de claves nuevo, y los datos de la copia de seguridad se vuelven a encriptar en estas claves nuevas. Tal como se ha explicado anteriormente, los ítems del llavero no migratorios permanecen encapsulados con la clave derivada del UID, lo cual hace posible su restauración en el dispositivo en el que se haya realizado la copia de seguridad original, pero impide el acceso a ellos en un dispositivo diferente.

El repositorio de claves está protegido con el conjunto de contraseñas establecido en iTunes, que se ejecuta en 10.000 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 muchos ordenadores tendrían lugar, teóricamente, en el repositorio de claves de copia de seguridad. Esta amenaza se puede mitigar con una contraseña suficientemente segura.

Si un usuario opta por no encriptar una copia de seguridad de iTunes, los archivos de copia de seguridad 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 ítems del llavero solo migran a un dispositivo nuevo cuando se establece una contraseña de copia de seguridad.

El repositorio de claves de custodia se utiliza para la sincronización con iTunes y MDM. Este repositorio de claves permite que iTunes realice una copia de seguridad y la sincronización sin necesidad de que el usuario introduzca un código, y permite que un servidor MDM borre de forma remota el código de un usuario. Se almacena en el ordenador utilizado para la sincronización con iTunes, o en el servidor MDM que gestiona el dispositivo.

El repositorio 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 introducir un código. Entonces, el dispositivo crea un repositorio 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 repositorio de claves de custodia y la clave que lo protege se reparten entre el dispositivo y el host o servidor; los datos almacenados en el dispositivo residen en la clase Protected Until First User Authentication. Por eso es necesario introducir el código del dispositivo antes de que el usuario realice la primera copia de seguridad con iTunes después de un reinicio.

Una instancia específica de un repositorio de claves de custodia, llamado *repositorio de claves intermedio*, se usa durante las actualizaciones de software para conceder al proceso de actualización acceso a los archivos e ítems del llavero con cualquier nivel de protección de datos. El acceso es necesario tras el reinicio del dispositivo durante el proceso de actualización para ejecutar los migradores de datos, que se ocupan de tareas como actualizar los esquemas de base de datos, generar previzualizaciones de ítems nuevos o incluso actualizar los niveles de la protección de datos.

En caso de una actualización de software OTA, el usuario tiene que introducir su código al inicio del proceso. Así, se establece de forma segura un indicador en el repositorio de claves del sistema que provoca la creación de un repositorio de claves intermedio en la memoria mientras el dispositivo está desbloqueado. Cuando el usuario está listo para realizar la actualización, que solo se puede llevar a cabo cuando el dispositivo está desbloqueado, se escribe en disco el repositorio de claves intermedio y se protege con una clave en Effaceable Storage. Al realizar la actualización con iTunes desde un host enlazado con un repositorio de claves de custodia válido, se solicita a los usuarios que desbloqueen su dispositivo antes de que empiece la actualización para permitir también la escritura en disco del repositorio de claves intermedio mientras el dispositivo está desbloqueado.

Cuando se ejecutan, los migradores de datos provocan la carga del repositorio de claves intermedio y, al hacerlo, conceden acceso a las claves de clase de protección de datos. En ese momento, se elimina el repositorio de claves intermedio almacenado en disco y la clave que lo protege se borra de Effaceable Storage para evitar que vuelva a usar. Cuando termina el proceso del migrador de datos, se descartan las claves que normalmente solo existen cuando el dispositivo está desbloqueado, y el dispositivo pasa a un estado posterior al primer desbloqueo.

Si no ha sido posible crear un repositorio de claves intermedio antes de la actualización, tras el reinicio del dispositivo, se muestra la indicación “Deslizar para actualizar” y se solicita el código para completar el proceso de actualización.

El repositorio de claves de copia de seguridad de iCloud es similar al de claves de copia de seguridad. Todas las claves de clase de este repositorio son asimétricas (utilizan Curve25519, como la clase de protección de datos Protected Unless Open), por lo que es posible realizar copias de seguridad 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, salvo para la clase No Protection. 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 las copias de seguridad de iTunes sin encriptar. También se utiliza un repositorio de claves asimétrico para la copia de seguridad en el aspecto de recuperación de llaveros de Llavero de iCloud.

FIPS 140-2

Los módulos cifrados en iOS 8 se están validando para garantizar su conformidad con las normas del Estándar federal de procesamiento de información de Estados Unidos (FIPS) 140-2 de nivel 1. Este proceso valida la integridad de las operaciones cifradas para apps de Apple y de terceros que utilicen correctamente los servicios cifrados de iOS. Para obtener más información acerca de las validaciones anteriores y el estado con respecto a iOS 8, consulte https://support.apple.com/kb/HT5808?viewlocale=es_ES.

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 gestionan bien, también pueden repercutir negativamente en la seguridad y estabilidad del sistema o en los datos de usuario.

Por esta razón, iOS añade 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 los 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 proceden de una fuente conocida y aprobada y 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 se deben validar y firmar con 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 aplicaciones 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 iOS. 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 todas las apps de 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.

iOS 8 permite a los desarrolladores incorporar en sus apps estructuras 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 a las que un proceso ofrezca un enlace al iniciarse. Esta verificación se consigue mediante el identificador de equipo (ID de equipo), 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 como ejecutable principal. Los ejecutables que se envían con el sistema no cuentan con un identificador de equipo, por lo que solo pueden contener enlaces a bibliotecas que se envíen con el propio sistema.

Las empresas también pueden crear apps internas para utilizarlas dentro de la organización y distribuirlas a sus empleados. Las empresas y organizaciones pueden solicitar el registro en el Programa Enterprise para desarrolladores de iOS (iDEP) con un número D-U-N-S. Apple aprueba las solicitudes tras verificar la identidad e idoneidad de los solicitantes. Una vez que una organización es miembro de iDEP, puede registrarse para obtener un perfil de datos que permita la ejecución de apps internas en los dispositivos autorizados. Los usuarios deben tener instalado el perfil de datos para poder ejecutar apps internas. De este modo, se garantiza que solo los usuarios que elija la organización pueden cargar las apps en sus dispositivos iOS. Las apps internas también comprueban la validez de la firma durante la ejecución. Aquellas que tengan un certificado caducado o revocado no se ejecutarán.

A diferencia de algunas 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 “aislan” para impedir su acceso 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, utiliza únicamente 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 solo lectura. Las herramientas innecesarias, 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 aplicación del sistema en peligro transfiera sus privilegios.

Además, las apps solo 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 mermados.

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 el caso de un ataque “return-to-libc” en el que 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, 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 activa 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. Solo 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, solo se puede realizar una llamada mmap para solicitar una página ejecutable y grabable, a la que se 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 emparejamiento.

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 emparejamiento específicas de cada punto de extensión. El sistema inicia los procesos de extensión automáticamente cuando es necesario y gestiona su duración. Las autorizaciones se pueden utilizar para restringir la disponibilidad de las extensiones a aplicaciones específicas del sistema. Por ejemplo, un widget de la vista Hoy solo aparece en el centro de notificaciones, y la extensión para compartir solo está disponible en el panel Compartir. Los puntos de extensión de Hoy son los widgets Compartir, “Acciones personalizadas”, “Edición de fotos”, “Proveedor de documentos” y “Teclado personalizado”.

Las extensiones se ejecutan en su propio espacio de direcciones. Para la comunicación entre la extensión y la app desde la que se ha activado, se utiliza la 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, 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 concede el acceso a Contactos a una app, 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 extensiones especial, que el usuario activa para todo el sistema. Una vez que se haya activado, la extensión se utilizará para cualquier campo de texto, salvo el de la introducción del código y cualquier vista de texto seguro. Por cuestiones de privacidad, los teclados personalizados se ejecutan por omisión 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 registre los datos introducidos. 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 por omisión tras obtener el consentimiento del usuario.

En el caso de los dispositivos inscritos en MDM, las extensiones de teclado y documentos obedecen a las reglas “Managed Open In”. Por ejemplo, el servidor MDM puede impedir que un usuario exporte un documento de una app gestionada a un proveedor de documentos sin gestionar o que utilice un teclado sin gestionar con una app gestionada. Además, los desarrolladores de aplicaciones pueden impedir el uso de extensiones de teclado de terceros en su aplicación.

Grupos de apps

Las apps y extensiones que son propiedad de una cuenta de desarrollador determinada pueden compartir contenido si se configuran como parte de un grupo de apps. Si así lo desea, el desarrollador puede crear los grupos adecuados en el Apple Developer Portal e incluir el conjunto deseado de apps y extensiones. Una vez que se han configurado como parte de un grupo de apps, las apps tienen acceso a lo siguiente:

- Un contenedor en disco compartido para el almacenamiento, que permanecerá en el dispositivo mientras al menos una de las apps del grupo esté instalada.
- Preferencias compartidas.
- Ítems del llavero compartidos.

El Apple Developer Portal 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 facilitan 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 API de archivo y de base de datos, como `NSFileManager`, `CoreData`, `NSData` y `SQLite`.

La app Mail (archivos adjuntos incluidos), los libros gestionados, las imágenes de inicio de las apps y los datos de ubicación también se almacenan encriptados con claves protegidas por el código del usuario en su dispositivo. Las apps Calendario (archivos adjuntos no incluidos), Contactos, Recordatorios, Notas, Mensajes y Fotos implementan la clase `Protected Until First User Authentication`.

Las apps instaladas por el usuario que no activan una clase de protección de datos específica reciben por omisión la clase `Protected Until First User Authentication`.

Accesorios

El programa de licencias Made for iPhone, iPod touch y iPad (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, que el dispositivo verifica, para 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 gestionado por un circuito integrado personalizado que Apple proporciona a los fabricantes de accesorios aprobados y es transparente para el accesorio.

Los accesorios pueden solicitar acceso a funcionalidades y métodos de transporte diferentes; 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 solo tienen acceso total al dispositivo los dispositivos aprobados. Si un accesorio no se autentica, su acceso queda limitado al audio analógico y a un pequeño subconjunto de controles de reproducción de audio 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 vídeo 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, y este 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 solo se incluyen en las copias de seguridad encriptadas 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 los ajustes originales 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 introduce en el dispositivo iOS y 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 se aplica tanto a los accesorios basados en IP como a los accesorios Bluetooth de baja energía.

Almacenamiento local de datos

HomeKit almacena datos sobre casas, accesorios, escenarios 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 nonce aleatorio. Además, los datos de HomeKit se almacenan con la clase de protección de datos Protected Until First User Authentication. Los datos de HomeKit solo se incluyen en copias de seguridad encriptadas; así, por ejemplo, las copias de seguridad 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 nonce aleatorio. Estos datos se gestionan 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 solo 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 añadir un usuario a una casa. Después de añadir un usuario nuevo a una casa, todas las comunicaciones se autentican y encriptan con el protocolo STS y claves por sesión.

Solo el usuario que creó el grupo de casa en HomeKit puede añadir usuarios nuevos. Su 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. El proceso de configuración del Apple TV para poder usarlo con HomeKit sigue el mismo procedimiento de autenticación y encriptación que la adición de usuarios nuevos, pero se realiza de forma automática si el usuario que creó el grupo de casa ha iniciado sesión en iCloud desde el Apple TV y el Apple TV se encuentra en la casa.

Si un usuario no tiene varios dispositivos ni 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 los ajustes 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.

Siri

Siri se puede utilizar para enviar consultas a los accesorios y controlarlos, y para activar escenarios. Tal como se describe en la sección sobre Siri de este documento, se envía muy poca información acerca de la configuración de la casa a Siri, y se hace de forma anónima. Esta información incluye los nombres de habitaciones, accesorios y escenarios que son necesarios para el reconocimiento de comandos.

HealthKit

La estructura de HealthKit proporciona una base de datos común que las apps pueden utilizar para almacenar datos de salud y forma física, y acceder a ellos, con el permiso del usuario. HealthKit funciona directamente con dispositivos de salud y forma física, como los monitores de frecuencia cardíaca Bluetooth de baja energía compatibles y el coprocesador de movimiento M7 o M8 integrado en muchos dispositivos iOS.

Datos de salud

HealthKit utiliza una base de datos para almacenar los datos de salud del usuario, como su altura, peso, distancia caminada, tensión arterial, etc. Esta base de datos se almacena en la clase de protección de datos Complete Protection, de modo que solo está accesible cuando el usuario introduce su código o utiliza Touch ID para desbloquear el dispositivo.

Otra base de datos almacena datos operativos, como tablas de acceso para apps, nombres de dispositivos conectados a HealthKit e información de programación utilizada para abrir apps cuando hay datos nuevos disponibles. Esta base de datos se almacena en la clase de protección de datos Protected Until First User Authentication.

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 Protected Unless Open. Cuando el dispositivo está desbloqueado, se importan en las bases de datos de salud principales y, una vez que ha terminado la fusión, se eliminan.

Los datos de salud no se comparten a través de iCloud ni se sincronizan con otros dispositivos. Las bases de datos de salud se incluyen en las copias de seguridad de dispositivos encriptadas que se realizan en iCloud o iTunes. Los datos de salud no se incluyen en las copias de seguridad de iTunes 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 aplicación que identifica la app que ha almacenado el registro. Además, otros metadatos opcionales pueden contener una copia del registro 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 cifrados (CMS) que se especifica en la RFC 5652 del IETF.

Acceso de aplicaciones de terceros

El acceso a la API de HealthKit se controla mediante autorizaciones; 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 con los ajustes de privacidad del usuario. Los usuarios tienen que conceder 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, las apps reciben acceso independiente para la lectura y escritura de datos, y para cada tipo de datos de salud. Los usuarios pueden ver y revocar los permisos que se les haya 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.

Datos médicos

La app Salud incorporada en iOS 8 permite a los usuarios rellenar un formulario con sus datos médicos e información que pueda ser importante durante una emergencia médica. La información se introduce o actualiza manualmente y no se sincroniza con la información de las bases de datos de salud.

Para ver la información de “Datos médicos”, basta con pulsar el botón SOS de la pantalla de bloqueo. La información se almacena en el dispositivo con la clase de protección de datos No Protection, de modo que se pueda acceder a ella sin necesidad de introducir el código del dispositivo. “Datos médicos” es una función opcional que permite a los usuarios decidir cómo conseguir un equilibrio entre seguridad y privacidad.

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 comprobadas y los estándares más recientes para conexiones de red de datos móviles y Wi-Fi.

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

SSL y TLS

iOS es compatible con los protocolos de capa de conexión segura (SSL 3), seguridad de la capa de transporte (TLS 1.0, TLS 1.1 y TLS 1.2) y DTLS. Safari, Calendario, Mail y otras apps de Internet utilizan estos mecanismos automáticamente 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.

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:

- Juniper Networks, Cisco, Aruba Networks, SonicWALL, Check Point, Palo Alto Networks, Open VPN, AirWatch, MobileIron, NetMotion Wireless y F5 Networks SSL-VPN si se utiliza la app cliente apropiada de la tienda App Store.
- Cisco IPsec con autenticación de usuario mediante contraseña, RSA SecurID o CRYPTOCARD, y autenticación de máquina mediante secreto compartido y certificados. Cisco IPsec es compatible con VPN por petición para los dominios especificados durante la configuración del dispositivo.
- L2TP/IPsec con autenticación de usuario mediante contraseña de MS-CHAPV2, RSA SecurID o CRYPTOCARD, y autenticación de máquina mediante secreto compartido.
- PPTP con autenticación de usuario mediante contraseña de MS-CHAPV2 y RSA SecurID o CRYPTOCARD.

iOS es compatible con “VPN por petición” para las redes que utilizan la autenticación basada en certificados. Las políticas de TI utilizan un perfil de configuración para especificar los dominios que requieren una conexión VPN.

iOS también admite la “VPN por app”, facilitando así las conexiones VPN de forma mucho más granular. Mobile Device Management (MDM) puede especificar una conexión para cada app gestionada o 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.

iOS 8 introduce el ajuste “VPN siempre activada”, que se puede configurar para dispositivos gestionados con MDM y que se supervisan con Apple Configurator o el Programa de inscripción de dispositivos. Así se elimina la necesidad de que los usuarios activen la red VPN para obtener protección al conectarse a redes Wi-Fi. El ajuste “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. Ahora 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 están 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.

iOS 8 utiliza una dirección de control de acceso al medio (MAC) aleatorizada al realizar exploraciones de preferencia de descarga de red (PNO) cuando un dispositivo no está asociado a una red Wi-Fi y su procesador está en reposo. El procesador de un dispositivo entra en reposo poco después de que se apague la pantalla. Las exploraciones PNO se ejecutan para determinar si un usuario se puede conectar a una red Wi-Fi preferida para realizar operaciones como la sincronización inalámbrica con iTunes.

iOS 8 también utiliza una dirección MAC aleatorizada 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 móvil.

Hemos trabajado con fabricantes de Wi-Fi para informarles de que las exploraciones en segundo plano utilizan una dirección MAC aleatorizada, pero ni Apple ni los fabricantes pueden predecir estas direcciones MAC aleatorias.

La aleatorización de direcciones MAC para Wi-Fi se admite en los iPhone 5c, 5s, 6 y 6 Plus, así como en el iPad Air y el iPad mini con pantalla Retina.

Bluetooth

El soporte para Bluetooth en iOS se ha diseñado 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 manos libres (HFP 1.5)
- Perfil de acceso a la agenda telefónica (PBAP)
- Perfil de distribución de audio avanzado (A2DP)
- Perfil de control remoto de audio/vídeo (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, consulte https://support.apple.com/kb/ht3647?viewlocale=es_ES.

Inicio de sesión único

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 en los que tienen autorización de acceso. El SSO se puede utilizar para diferentes operaciones de red, desde la navegación segura en Safari hasta el uso de aplicaciones de terceros.

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 tickets de Kerberos. También admite la autenticación basada en certificados. 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 las apps de terceros que utilizan API de conexión a redes de iOS estándar también se pueden configurar para que lo hagan. Para configurar el SSO, iOS admite una carga de perfil de configuración que permite a los servidores MDM obtener los ajustes necesarios. Aquí se incluye el nombre del principal usuario (es decir, la cuenta de usuario de Active Directory) y los ajustes del reino Kerberos, así como la configuración de las apps o 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 los ordenadores Mac compatibles con AirDrop que ejecuten OS X Yosemite. 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 ID de Apple del usuario.

Cuando un usuario elige AirDrop como método para compartir un ítem, 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.

El ajuste por omisión de AirDrop para compartir es “Solo contactos”. Los usuarios también pueden indicar si desean poder utilizar AirDrop para compartir con Todos o desactivar la función por completo. En el modo “Solo 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 han seleccionado 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 y el nombre del dispositivo, tal como se indica en Ajustes > General > Información > Nombre.

Servicios de Internet

Creación de contraseñas seguras de ID de Apple

Los ID de Apple 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 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 debe contener más de tres caracteres idénticos consecutivos,
- no debe coincidir con el nombre de la cuenta.

Apple ha creado 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, Siri, sugerencias de Spotlight, iCloud, copia de seguridad de iCloud y llavero de iCloud.

Estos servicios de Internet se han diseñado con los mismos objetivos de seguridad que iOS promueve en toda su plataforma. Dichos objetivos incluyen la gestión 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 comprometer la facilidad de uso global de iOS.

ID de Apple

El ID de Apple está constituido por el nombre y la contraseña del usuario necesarios para iniciar sesión en servicios de Apple tales como iCloud, iMessage, FaceTime, iTunes Store, iBooks Store y App Store entre otros. Es importante que el usuario proteja su ID de Apple para evitar que se produzca un acceso no autorizado a sus cuentas. Con el fin de ayudarle 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 añadiendo más caracteres o signos de puntuación para que sus contraseñas resulten aún más seguras. 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 ha modificado una contraseña o la información de facturación, o bien si el ID de Apple se ha utilizado para iniciar sesión en un dispositivo nuevo. Si los usuarios detectan algo que no les resulta familiar, deben cambiar la contraseña de su ID de Apple inmediatamente.

Asimismo, Apple ofrece una verificación del ID de Apple que se realiza en dos pasos y proporciona una segunda capa de seguridad para la cuenta del usuario. 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 ningún cambio en la información de la cuenta de su ID de Apple, iniciar sesión en iCloud o realizar compras en iTunes Store, iBooks Store o App Store desde un dispositivo nuevo. Así se evita el acceso de cualquier persona a la cuenta del usuario incluso si esa persona conoce la contraseña. 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.

Si desea obtener más información sobre la verificación en dos pasos del ID de Apple, visite https://support.apple.com/kb/ht5570?viewlocale=es_ES.

iMessage

iMessage de Apple es un servicio de mensajería para dispositivos iOS y ordenadores 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 mensajes ni archivos adjuntos y su contenido está protegido mediante una encriptación de punto a punto, de modo que únicamente el emisor y el receptor pueden acceder a ellos, ya que Apple no puede descryptar 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 APNs del dispositivo.

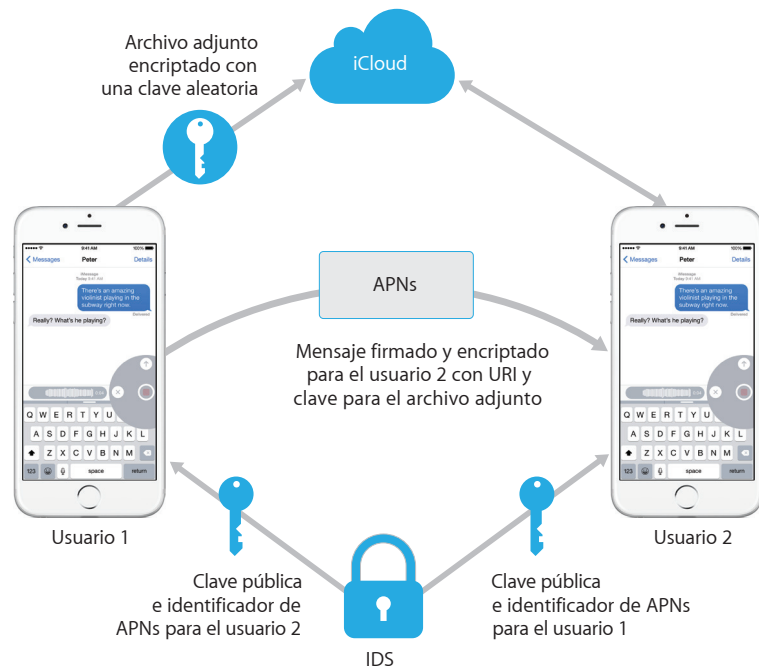
A medida que los usuarios activan otros dispositivos para usarlos con iMessage, las claves públicas de encriptación y firma, las direcciones del APNs y los números de teléfono asociados se añaden al servicio de directorio. Los usuarios también pueden añadir más direcciones de correo electrónico, que se verificarán mediante el envío de un enlace de confirmación. La SIM y la red del operador verifican los números de teléfono. Además, en todos los dispositivos registrados del usuario, se muestra un mensaje de aviso al añadir un dispositivo, número de teléfono o dirección de correo electrónico nuevos.

Cómo envía y recibe mensajes iMessage

Los usuarios inician una nueva conversación de iMessage al introducir una dirección o un nombre. Si introducen 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 introduce 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, a continuación, obtiene las claves públicas y las direcciones del APNs del IDS de Apple.

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 una clave aleatoria de 128 bits que utiliza para encriptar el mensaje con AES en modo CTR. 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.

El APNs solo puede transmitir mensajes de 4 o 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. A continuación, 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 a continuación.



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 necesario, recupera 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, a ser 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 la cola para enviarlos a los dispositivos sin conexión. Actualmente los mensajes se almacenan durante quince días como máximo, pero se pretende ampliar ese plazo de tiempo a treinta días en un futuro próximo.

FaceTime

FaceTime es el servicio de llamadas de audio y vídeo 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/vídeo de las llamadas FaceTime se protege mediante la encriptación de punto a punto, con lo cual, únicamente el emisor y el receptor pueden acceder a él ya que Apple no puede desencriptar los datos.

FaceTime utiliza el establecimiento de conectividad de Internet (ICE) para establecer una conexión P2P entre los dispositivos. Al usar mensajes conforme al Protocolo de inicio de sesión (SIP), los dispositivos verifican sus certificados de identidad y establecen un secreto compartido para cada sesión. Los nonces cifrados que suministra cada dispositivo se combinan con claves de sal para cada uno de los canales de contenido multimedia, que se transmiten mediante el Protocolo en tiempo real seguro (SRTP) con la encriptación AES-256.

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 valores de clave para datos de apps según las indicaciones del desarrollador. Los usuarios configuran iCloud al iniciar sesión con un ID de Apple y seleccionar qué servicios desean usar. Los administradores de TI pueden desactivar funciones de iCloud tales como “Mis fotos en streaming”, iCloud Drive y la copia de seguridad de iCloud mediante un perfil de configuración. El servicio no reconoce qué se está almacenando y gestiona 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 identificativa del usuario) mediante servicios de almacenamiento de terceros como Amazon S3 y Microsoft Azure.

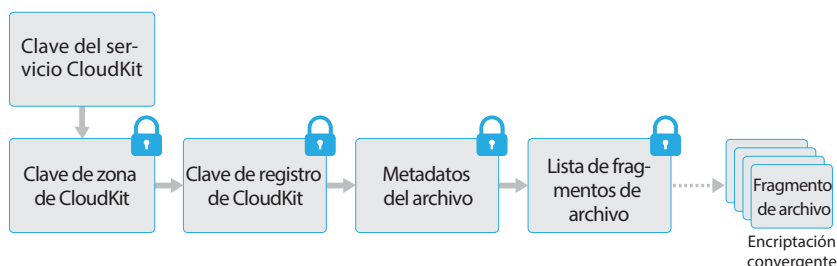
iCloud Drive

iCloud Drive añade claves basadas en las cuentas para proteger documentos almacenados en iCloud. Tal como sucede con los servicios de iCloud existentes, este servicio fragmenta y encripta el contenido de los archivos y, a continuación, 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, a continuación, dicha clave de servicio se almacena con la cuenta de iCloud del usuario. Tras 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.

CloudKit

CloudKit permite a los desarrolladores de apps almacenar datos 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 mediante 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 solo está disponible una vez que el usuario se ha autenticado con iCloud.



Copia de seguridad de iCloud

iCloud también realiza copias de seguridad de información (como ajustes de los dispositivos, datos de las apps, fotos y vídeos en Carrete, 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. Las copias de seguridad de iCloud se llevan a cabo únicamente cuando el dispositivo está bloqueado, conectado a una fuente de alimentación y con acceso a Internet mediante Wi-Fi. Debido a la encriptación que se usa en iOS, el sistema se ha diseñado para mantener protegidos los datos y, al mismo tiempo, permitir que se realicen copias de seguridad y restauraciones progresivas y sin supervisión.

A continuación, se indica el contenido del que iCloud realiza copias de seguridad:

- información sobre música, películas, programas de TV, apps y libros comprados, pero no sobre el contenido de la compra en sí mismo;
- fotos y vídeos almacenados en Carrete;
- contactos, eventos de calendario, recordatorios y notas;
- ajustes de los dispositivos;
- datos de las apps;
- archivos PDF y libros que se han añadido a iBooks, pero que no se han comprado;
- historial de llamadas;
- organización de la pantalla de inicio y las apps;
- mensajes de iMessage, mensajes de texto (SMS) y mensajes MMS;

- tonos de llamada;
- datos de HomeKit;
- datos de HealthKit;
- buzón de voz visual.

Cuando los archivos se crean en clases de protección de datos a las que no se puede acceder cuando el archivo está bloqueado, las claves por archivo correspondientes se encriptan con las claves de clase del repositorio de claves de copia de seguridad de iCloud. Las copias de seguridad en iCloud de los archivos se realizan en su estado encriptado original. Los archivos en la clase de protección de datos No Protection se encriptan durante el transporte.

El repositorio de claves de copia de seguridad de iCloud contiene claves asimétricas (Curve25519) para cada clase de protección de datos. Estas claves asimétricas se usan para encriptar las claves por archivo. Si desea obtener más información acerca del contenido de los repositorios de claves de copia de seguridad y de copia de seguridad de iCloud, consulte el apartado “Protección de datos de llavero” de la sección “Encriptación y protección de datos”.

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

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

Al restaurarlo, los archivos de los que se ha realizado la copia de seguridad, el repositorio de claves de copia de seguridad de iCloud y la clave para el repositorio de claves se recuperan de la cuenta de iCloud del usuario. El repositorio de claves de copia de seguridad de iCloud se desencripta usando su clave, a continuación, las claves por archivo del repositorio de claves se usan para desencriptar los archivos del conjunto de copias de seguridad, 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.

Llavero de iCloud

El llavero de iCloud permite a los usuarios sincronizar de forma segura sus contraseñas entre dispositivos iOS y ordenadores Mac sin exponer esa 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 llavero para que las contraseñas del usuario se mantuvieran protegidas en las siguientes circunstancias:

- La cuenta de iCloud de un usuario está en peligro.
- iCloud está en peligro a causa de un ataque o empleado externos.
- Terceras personas acceden a las cuentas del usuario.

Integración de Safari con el llavero de iCloud

Safari puede generar, automáticamente y mediante cifrado, cadenas seguras aleatorias para contraseñas de sitios web, que se almacenan en el llavero y se sincronizan con el resto de sus dispositivos. Los ítems 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.

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 P256) derivada de la contraseña de la cuenta de iCloud del usuario. Junto con el círculo, se almacenan los parámetros (salt 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, el nuevo dispositivo detecta en iCloud que el usuario dispone de un círculo de sincronización previo establecido al que no pertenece. El dispositivo crea el par de claves de identidad de sincronización correspondiente y, a continuación, crea un vale de aplicación para solicitar formar parte de ese círculo como miembro. El vale 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 recuperan de iCloud y se genera una clave que se usa para firmar el tique de aplicación. Por último, este vale se coloca en iCloud.

Cuando el primer dispositivo detecta la recepción de un tique 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 introduce su contraseña de iCloud, y se comprueba que el tique de aplicación está firmado por una clave privada coincidente. Esto determina que la persona que ha generado la solicitud para entrar en el círculo ha introducido la contraseña de iCloud del usuario cuando se le ha solicitado.

Tras la aprobación del usuario para añadir un dispositivo nuevo al círculo, el primer dispositivo añade la clave pública del nuevo miembro al círculo de sincronización, 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 ítems individuales del llavero mediante el almacenamiento de datos clave-valor de iCloud. Si ambos miembros del círculo disponen del mismo ítem, se sincronizará el de la fecha de modificación más reciente. Los ítems se ignorarán en el caso de que el otro miembro también los tenga con la misma fecha de modificación. Cada ítem que se sincroniza se encripta de forma específica para el dispositivo al que se envía. Ni Apple ni otros dispositivos pueden desencriptarlo. Además, el ítem encriptado es efímero en iCloud: se sobrescribe con cada ítem nuevo que se sincronice.

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 añadir nuevos dispositivos, cada uno se sincroniza con el nuevo para garantizar que todos los miembros disponen de los mismos ítems en el llavero.

Sin embargo, no se sincroniza todo el llavero. Algunos ítems, como las identidades de VPN, son específicos de cada dispositivo y no deben abandonarlo. Solo se sincronizan los ítems con el atributo `kSecAttrSynchronizable`. Apple ha configurado ese 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, por omisión, los ítems del llavero que hayan añadido apps de terceros no se sincronizan. Los desarrolladores deben definir el atributo `kSecAttrSynchronizable` al añadir ítems al llavero.

Recuperación del llavero

La recuperación del llavero es una posibilidad para los usuarios 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.

Cuando se enciende el llavero de iCloud, se solicita al usuario que cree un código de seguridad de iCloud. Este código es necesario para recuperar el llavero custodiado. Por omisión, se solicita al usuario que proporcione un valor de cuatro dígitos sencillo para el código de seguridad. Sin embargo, los usuarios también pueden especificar su propio código, que puede ser más largo, o bien permitir que sus dispositivos generen un código aleatorio cifrado, que pueden registrar y guardar.

A continuación, el dispositivo iOS exporta una copia del llavero del usuario, lo encripta encapsulado con claves en un repositorio de claves asimétrico y lo coloca en el área de almacenamiento de datos clave-valor de iCloud del usuario. El repositorio 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 aleatorio cifrado en lugar de especificar el suyo 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 proporcionará 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 solo los usuarios y los dispositivos autorizados pueden realizar una recuperación. Detrás de iCloud, hay clústeres de Hardware Security Modules (HSM) que protegen 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 ha descrito anteriormente.

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 introducir su código de seguridad de iCloud. El clúster de HSM verifica que el usuario conoce el código de seguridad de iCloud, que no se envía a Apple, mediante el protocolo de contraseña remota segura (SRP). Cada miembro del clúster verifica de manera independiente que el usuario no ha superado el número máximo de intentos que se permite 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. Solo se permiten 10 intentos para autenticar y recuperar un registro de la custodia. Tras 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. Tras el 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 los ataques de fuerza bruta para intentar 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, los propietarios de todos los llaveros a los que protege el clúster recibirán un mensaje en el que se indicará que el registro de la custodia se ha perdido. 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 se han diseñado para garantizar que solamente se utiliza la cantidad mínima de información personal y que está 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.

Al iniciar sesión en Siri, el nombre y el apellido del usuario (obtenidos de Contactos) se envían al servidor junto con una ubicación geográfica aproximada con el fin de que Siri pueda responder con el nombre o responder a las consultas para las que solo sea necesario conocer la ubicación aproximada como, por ejemplo, las relacionadas con la previsión meteorológica.

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, por omisión, solo 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 tras 10 minutos de inactividad.

La grabación de las palabras pronunciadas por el usuario se envía al servidor de reconocimiento de voz de Apple. Si la tarea solo consiste en un dictado, el texto reconocido se envía de vuelta 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 mi madre”, 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 de servidor. Por ejemplo, si el usuario le pide a Siri que lea un mensaje que ha 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. 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.

Siri también se puede invocar en modo manos libres mediante la activación por voz. La detección del activador de 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 concreta del activador. Cuando se detecta el activador, 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.

Continuity

Continuity, novedad de iOS 8 y OS X Yosemite, 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, así como compartir la conexión a Internet de un dispositivo móvil.

Handoff

Con Handoff, cuando el Mac y el dispositivo 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 APNs. Los mensajes individuales están encriptados de forma similar a como sucede en iMessage. Una vez que los dispositivos están

enlazados, cada uno generara una clave simétrica AES de 256 bits que se almacena en el llavero del dispositivo. Esta clave se usa para 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 el 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, así como mediante la encriptación de los mensajes individuales, que es parecida a la encriptación de iMessage. En algunas situaciones, estos mensajes se envían mediante el servicio de notificaciones push de Apple 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 que se usa para credenciales web compartidas. Si desea obtener más información, consulte el apartado “Acceso a contraseñas guardadas en Safari” en la sección “Encriptación y protección de datos”. 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 ha descrito previamente en la sección anterior).

En un dispositivo receptor, el sistema detecta que una app nativa instalada acepta Handoff desde el nombre de dominio anunciado y muestra el icono 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 por omisión 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, tras 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.

Transmisión de llamadas telefónicas del iPhone

Si el Mac, el iPad o el iPod están conectados a la misma red Wi-Fi que el iPhone, podrán realizar y recibir llamadas telefónicas con la conexión de telefonía móvil del iPhone. La configuración requiere que los dispositivos hayan iniciado sesión tanto en iCloud como en FaceTime con la misma cuenta de ID de Apple.

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

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 transferencia de llamadas telefónicas en un dispositivo desactivando “Llamadas telef. del iPhone” en los ajustes 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 el 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 ID de Apple. Cuando esta opción se activa, el iPhone genera un código numérico de seis dígitos aleatorio que se introduce 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, a continuación, el iPhone las envía como mensajes de texto con ayuda del mecanismo de transmisión de SMS del operador. La opción “Reenvío de mensajes de texto” se puede desactivar en los ajustes 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. Los ordenadores Mac en los que se ejecute el sistema operativo OS X Yosemite utilizan la misma tecnología para detectar dispositivos iOS y comunicarse con ellos mediante Instant Hotspot.

Cuando un usuario abre “Ajustes 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 vinculado a la cuenta de iCloud y va rotando periódicamente. Si hay otros dispositivos que han iniciado sesión en la misma cuenta de iCloud cerca y son compatibles con la función de compartir Internet, detectan la señal y responden 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 Spotlight

Ahora, las búsquedas de Safari y de Spotlight incluyen sugerencias de Spotlight, que proporcionan sugerencias de búsquedas en Internet, iTunes, App Store, la cartelera de cine, ubicaciones cercanas y mucho más.

Para conseguir que las sugerencias sean más pertinentes para el usuario, las sugerencias de Spotlight incluyen el contexto del usuario y los comentarios sobre la búsqueda con las solicitudes de consulta de búsqueda enviadas a Apple.

El contexto enviado con las solicitudes de búsqueda indican a Apple: i) la ubicación aproximada del dispositivo; ii) el tipo de dispositivo (p. ej., el Mac, el iPhone, el iPad o el iPod); iii) la app cliente (que es Spotlight o Safari); iv) los ajustes por omisión de idioma y región del dispositivo; v) las tres apps usadas más recientemente en el dispositivo; y vi) un ID de sesión anónimo. Toda la comunicación con el servidor se encripta mediante el protocolo HTTPS.

Con el fin de ayudar a proteger la privacidad del usuario, las sugerencias de Spotlight nunca proporcionan una ubicación exacta, sino una ubicación aproximada en la app cliente antes de enviarla. El grado de aproximación se basa en la densidad de población estimada en la ubicación del dispositivo; por ejemplo, en un entorno rural la aproximación usada será menor que en el caso del centro de una ciudad donde, normalmente, los usuarios estarán más cerca unos de otros. Además, los usuarios pueden desactivar el envío a Apple de toda información relacionada con la ubicación en Ajustes si desactivan la función Localización para las sugerencias de Spotlight. En ese caso, Apple puede usar la dirección IP del cliente para deducir una ubicación aproximada.

El ID de sesión anónimo permite a Apple analizar patrones entre las consultas realizadas en un periodo de tiempo de 15 minutos. Por ejemplo, si los usuarios buscan frecuentemente “Número de teléfono de la cafetería” poco tiempo después de buscar “Cafetería”, puede que Apple entienda que deba incluir con más frecuencia el número de teléfono en los resultados. A diferencia de la mayoría de los motores de búsqueda, el servicio de búsqueda de Apple no utiliza siempre el mismo identificador personal durante todo el historial de búsqueda de un usuario para relacionar las consultas con un usuario o dispositivo. Por el contrario, los dispositivos de Apple usan un ID de sesión anónimo temporal durante un periodo máximo de 15 minutos antes de descartar ese ID.

La información de las tres últimas apps que se han usado en el dispositivo se incluye como contexto de búsqueda adicional. Con el fin de proteger la privacidad de los usuarios, solo se incluyen apps que figuren en la lista blanca de Apple de apps populares a las que se haya accedido durante las últimas tres horas.

Los comentarios sobre la búsqueda que se envían a Apple proporcionan a Apple: i) información sobre el tiempo que transcurre entre las acciones del usuario como las pulsaciones de las teclas y las selecciones de los resultados; ii) los resultados seleccionados de las sugerencias de Spotlight, si se ha seleccionado alguno; y iii) el tipo de resultado local seleccionado (p. ej., Marcador o Contacto). Tal y como sucede con el contexto de búsqueda, el comentario de la búsqueda no está vinculado a ninguna persona o dispositivo individual.

Apple guarda registros de las sugerencias de Spotlight con las consultas, el contexto y los comentarios durante un máximo de 18 meses. Los registros reducidos que incluyen únicamente una consulta, el idioma, la fecha (hora) y el tipo de dispositivo se guardan hasta dos años. Las direcciones IP no se guardan con los registros de las consultas.

En algunos casos, las sugerencias de Spotlight pueden remitir las consultas sobre palabras y frases comunes a un socio cualificado para recibir y mostrar los resultados de la búsqueda de dicho socio. Los socios cualificados no almacenan esas consultas y ni reciben los comentarios sobre las búsquedas. Además, tampoco reciben las direcciones IP del usuario. La comunicación con los socios se encripta mediante el protocolo HTTPS. Apple proporciona a los socios información sobre la ubicación (la ciudad), el tipo de dispositivo y el idioma de la app cliente como contexto de búsqueda en función de los que Apple detecta que se repiten en las consultas.

Las sugerencias de Spotlight se pueden desactivar en los ajustes de Spotlight, Safari o ambos. Si se desactivan en los ajustes de Spotlight, Spotlight volverá a convertirse en una app cliente que solo realizará búsquedas locales en el dispositivo y que no transmitirá información a Apple. Si se desactivan en los ajustes de Safari, las consultas de búsqueda del usuario, el contexto de búsqueda y el comentario de la búsqueda no se transmitirán a Apple.

Controles del dispositivo

iOS es compatible con políticas de seguridad y configuraciones flexibles que se pueden aplicar y gestionar fácilmente. Gracias a estas políticas, las organizaciones pueden proteger su información corporativa y garantizar que sus empleados cumplen con los requisitos de la empresa, incluso si utilizan sus propios dispositivos, por ejemplo, como parte de un programa “traiga su propio dispositivo” (BYOD).

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

Protección mediante código

Además de proporcionar la protección criptográfica indicada anteriormente, los códigos impiden el acceso no autorizado a la IU del dispositivo. La interfaz de iOS aplica tiempos de demora cada vez mayores tras la introducción de un código no válido, de forma que se reduce notablemente la eficacia de los ataques de fuerza bruta realizados en pantalla de bloqueo. Si lo desean, los usuarios pueden configurar el dispositivo para que su contenido se borre automáticamente tras 10 intentos fallidos de introducir el código correcto. Este ajuste está disponible como política de administración y también se puede definir con un umbral inferior a través de los perfiles de configuración, MDM y Exchange ActiveSync.

Por omisión, el código del usuario se puede definir como un PIN de cuatro dígitos. Los usuarios pueden especificar un código alfanumérico más largo en Ajustes > General > Código > Código complejo. Los códigos más largos y más complejos son más difíciles de averiguar o atacar y se recomiendan para el uso empresarial.

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 para el bloqueo automático agotado.
- Periodo de gracia para el bloqueo del dispositivo.
- Número máximo de intentos fallidos.
- Permitir Touch ID.

Si desea obtener más información sobre cada política, consulte la documentación sobre la referencia de la clave del perfil de configuración en <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 un ordenador 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.

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. Una vez hecho esto, el host y el dispositivo intercambian y guardan claves públicas RSA de 1024 bits. A continuación, el host recibe una clave de 256 bits con la que puede desbloquear un repositorio de claves de custodia almacenado en el dispositivo (véase la información sobre los repositorios de claves de custodia en la sección “Repositorios de claves”). 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.). A fin de utilizar esta sesión encriptada para todas las comunicaciones, el dispositivo precisa conexión desde un host a través de la red Wi-Fi, con lo cual, debe enlazarse previamente mediante USB. Además, el enlace también activa varias funciones de diagnóstico. Si desea obtener más información, consulte https://support.apple.com/kb/HT6331?viewlocale=es_ES.

En iOS, determinados servicios como com.apple.pcapd solo pueden funcionar mediante USB. Además, en iOS 8, el servicio com.apple.file_relay precisa la instalación de un perfil de configuración firmado por Apple.

El usuario puede borrar la lista de hosts de confianza con las opciones “Restablecer ajustes de red” o “Restablecer localización y privacidad”. Si desea obtener más información, consulte https://support.apple.com/kb/HT5868?viewlocale=es_ES.

Aplicación de la configuración

Un perfil de configuración es un archivo XML que permite que un administrador distribuya información relacionada con la configuración a dispositivos iOS. El usuario no puede modificar los ajustes definidos mediante un perfil de configuración instalado. Si el usuario elimina un perfil de configuración, también se eliminan todos los ajustes que lo definen. De este modo, los administradores pueden aplicar ajustes mediante la vinculación de las políticas al acceso. Por ejemplo, un perfil de configuración que proporciona una configuración de correo electrónico también puede especificar una política de código del dispositivo. Los usuarios solo podrán acceder al correo electrónico si sus códigos cumplen los requisitos del administrador.

Un perfil de configuración de iOS contiene una serie de ajustes que se pueden especificar, incluidos los siguientes:

- políticas de código;
- restricciones en las funciones del dispositivo (por ejemplo, la desactivación de la cámara);
- ajustes de Wi-Fi;
- ajustes de VPN;
- ajustes del servidor de Mail;
- ajustes de Exchange;

- ajustes del servicio de directorio LDAP;
- ajustes del servicio de calendario CalDAV;
- clips web;
- credenciales y claves;
- ajustes avanzados de la red de telefonía móvil.

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 mediante 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. Como muchos usuarios empresariales disponen de su propio dispositivo iOS, los perfiles de configuración que unen un dispositivo a un servidor MDM se pueden eliminar. Sin embargo, al hacerlo, se eliminará también toda la información de configuración, las apps y los datos gestionados.

Los usuarios pueden instalar perfiles de configuración directamente en sus dispositivos mediante Apple Configurator, o bien pueden ser descargados con Safari, enviados mediante un mensaje de correo electrónico o de forma remota con ayuda de un servidor MDM.

Mobile Device Management (MDM)

La compatibilidad de iOS con MDM permite que las empresas puedan configurar y gestionar de forma segura la implantación gradual de iPhone y iPad en sus organizaciones. Las funciones de MDM están integradas en tecnologías iOS existentes tales como los perfiles de configuración, la inscripción remota y el servicio de notificaciones push de Apple (APNs). Por ejemplo, el servicio APNs se utiliza para activar los dispositivos de modo que se puedan comunicar directamente con el servidor MDM correspondiente mediante una conexión segura. A través de los servicios APNs, no se transmite información confidencial ni privada.

Con ayuda de MDM, los departamentos de TI pueden inscribir dispositivos iOS en un entorno empresarial, configurar los ajustes y actualizarlos mediante una red inalámbrica, supervisar el cumplimiento de políticas corporativas e incluso borrar o bloquear de forma remota los dispositivos gestionados. Si desea obtener más información sobre la gestión de dispositivos móviles, consulte www.apple.com/iphone/business/it/management.html.

Programa de inscripción de dispositivos

El Programa de inscripción de dispositivos (DEP) es una alternativa rápida y sencilla para implementar los dispositivos iOS que una organización compre directamente de Apple. La organización puede inscribir automáticamente dispositivos en MDM sin tener que tocarlos físicamente ni prepararlos antes de que los usuarios los reciban. 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 marcha rápidamente. Además, los administradores también pueden controlar si los usuarios pueden eliminar o no el perfil de MDM de los dispositivos. Por ejemplo, pueden encargar los dispositivos a Apple, configurar todos los ajustes de gestión y solicitar que los dispositivos se envíen directamente a la dirección postal del usuario. Una vez que el dispositivo se saca del embalaje y se activa, dicho dispositivo se inscribe en el servidor MDM de la organización, de manera que todos los ajustes de gestión, apps y libros ya están listos para el usuario.

El proceso es sencillo: Tras inscribirse en el programa, los administradores inician sesión en el sitio web del programa, enlazan el programa a su servidor MDM y “reclaman” los dispositivos iOS adquiridos a Apple. A continuación, los dispositivos se pueden asignar a los usuarios mediante el servidor MDM. Una vez que al usuario se le ha asignado un dispositivo, todas las configuraciones, restricciones o controles específicos de MDM se instalan automáticamente. Si desea obtener más información, consulte <https://deploy.apple.com>.

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

Apple Configurator

Además de MDM, Apple Configurator para OS X facilita a todo el mundo la implantación de dispositivos iOS. Apple Configurator se puede utilizar para configurar rápidamente un gran número de dispositivos con sus ajustes, apps y datos. Los dispositivos que se hayan configurado inicialmente con Apple Configurator se pueden “supervisar” y, con ello, permitir la instalación de configuraciones y restricciones adicionales. Tras supervisar un dispositivo con Apple Configurator, todos los ajustes y restricciones disponibles también se pueden instalar remotamente mediante el servidor MDM.

Si desea obtener más información acerca de la configuración y la gestión de dispositivos con MDM o Apple Configurator, consulte “Guía de referencia sobre la implantación de iOS” en <https://help.apple.com/deployment/ios>.

Restricciones del dispositivo

Mediante la instalación de un perfil de configuración, los administradores pueden restringir las funciones del dispositivo. Las siguientes restricciones están disponibles:

- Permitir instalar aplicaciones.
- Permitir usar la cámara.
- Permitir FaceTime.
- Permitir las capturas de pantalla.
- Permitir la marcación por voz.
- Permitir la sincronización automática en itinerancia.
- Permitir las compras desde apps.
- Permitir la sincronización de mensajes de Mail recientes.
- Obligar al usuario a introducir una contraseña para todas las compras.
- Permitir los juegos multijugador.
- Permitir añadir amigos de Game Center.
- Permitir Siri.
- Permitir Siri mientras el dispositivo está bloqueado.
- Permitir el uso de YouTube.
- Permitir las notificaciones de Passbook mientras el dispositivo está bloqueado.
- Permitir usar iTunes Store.
- Permitir el contenido multimedia explícito.
- Permitir la literatura erótica en iBooks Store.
- Permitir documentos de fuentes gestionadas en destinos no gestionados.
- Permitir documentos de fuentes no gestionadas en destinos gestionados.
- Permitir el llavero de iCloud.

- Permitir la actualización de la base de datos de confianza de certificados de forma remota.
- Permitir mostrar notificaciones en la pantalla de bloqueo.
- Forzar que las conexiones de AirPlay usen contraseñas de enlace.
- Permitir que Spotlight muestre contenido generado por el usuario de Internet.
- Activar las sugerencias de Spotlight en Safari.
- Activar las sugerencias de Spotlight en Spotlight.
- Permitir Handoff.
- Permitir realizar copias de seguridad de libros empresariales.
- Permitir que las notas y los marcadores de los libros empresariales se sincronicen en todos los dispositivos del usuario.
- Restringir las puntuaciones de las películas.
- Restringir las puntuaciones de TV.
- Restringir las puntuaciones de apps.
- Permitir usar Safari.
- Activar el autorrelleno en Safari.
- Forzar la advertencia de sitios web fraudulentos.
- Activar JavaScript.
- Limitar el seguimiento de anuncios en Safari.
- Bloquear las ventanas.
- Aceptar las cookies.
- Permitir la copia de seguridad de iCloud.
- Permitir la sincronización de documentos de iCloud y de datos clave-valor.
- Permitir las fotos en streaming.
- Permitir las secuencias de fotos compartidas.
- Permitir el envío de diagnósticos a Apple.
- Permitir que el usuario acepte certificados TLS que no sean de confianza.
- Forzar las copias de seguridad encriptadas.
- Restringir el contenido multimedia mediante la clasificación del contenido.
- Permitir Touch ID.
- Permitir el acceso al centro de control desde la pantalla de bloqueo.
- Permitir la vista Hoy desde la pantalla bloqueada.

Restricciones solo supervisadas

- Permitir iMessage.
- Permitir Game Center.
- Permitir iBooks Store.
- Permitir la eliminación de apps.
- Activar el filtro de palabrotas de Siri.
- Permitir la instalación manual de perfiles de configuración.
- Proxy de red global para HTTP.
- Permitir el enlace a ordenadores para sincronizar el contenido.
- Restringir las conexiones de AirPlay con la lista blanca y códigos de conexión opcionales.
- Permitir AirDrop.
- Permitir Podcasts.
- Permitir la modificación de Buscar a mis amigos.
- Permitir el modo de aplicación única autónoma para determinadas apps gestionadas.
- Permitir la modificación de la cuenta.
- Permitir la modificación de los datos móviles.
- Permitir el enlace del host (iTunes).
- Permitir el bloqueo de activación.
- Evitar "Borrar contenidos y ajustes".
- Evitar la activación de restricciones.
- Filtro del contenido de terceros.
- Modo de aplicación única.
- VPN siempre activada.

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 dejan de poder leerse. 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 Ajustes. Por último, como se ha mencionado anteriormente, los dispositivos se pueden configurar para que se realice un borrado automático del contenido tras una serie de intentos fallidos de introducir el código.

Buscar mi iPhone y Bloqueo de activación

En caso de pérdida o robo de un dispositivo, es importante desactivarlo y eliminar su contenido. Con iOS 7 o posterior, al activar Buscar mi iPhone, el dispositivo no se puede reactivar sin introducir las credenciales del ID de Apple del propietario. Es una buena idea que las organizaciones supervisen sus dispositivos o dispongan de una política para que los usuarios desactiven la función de forma que Buscar mi iPhone no impida que la organización le asigne el dispositivo a otra persona.

Con iOS 7.1 o posterior, una solución MDM compatible puede activar el bloqueo de activación en dispositivos supervisados cuando un usuario activa Buscar mi iPhone. Los administradores de MDM pueden gestionar la opción de bloqueo de activación de Buscar mi iPhone al supervisar dispositivos con Apple Configurator o con el Programa de inscripción de dispositivos. La solución MDM puede almacenar un código de anulación cuando el bloqueo de activación está activado y, después, usar este código para eliminar automáticamente el bloqueo si se tiene que borrar el contenido de un dispositivo para asignárselo a otro usuario. Si desea obtener más información, consulte la documentación de soluciones MDM.

Importante: por omisión, los dispositivos supervisados nunca tienen el bloqueo de activación activado, incluso aunque el usuario active Buscar mi iPhone. Sin embargo, un servidor MDM puede recuperar un código de anulación y permitir el bloqueo de activación en el dispositivo. Si Buscar mi iPhone está encendido cuando el servidor MDM permite el bloqueo de activación, se activará en ese momento. Si Buscar mi iPhone está apagado cuando el servidor MDM activa el bloqueo de activación, se activará la próxima vez que el usuario active Buscar mi iPhone.

Controles de privacidad

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

Localización

Para determinar la ubicación aproximada del usuario, se utiliza información del GPS y Bluetooth, junto con los datos de antenas de telefonía móvil y puntos activos de conexión Wi-Fi. La función Localización se puede desactivar con un sencillo cambio en Ajustes. Asimismo, los usuarios pueden aprobar el acceso para cada app que usa este servicio. Puede que algunas apps soliciten recibir datos de ubicación solo durante el uso de la app o que permitan la recepción en cualquier momento. Si lo desean, los usuarios pueden no permitir este acceso y pueden cambiar su elección en cualquier momento mediante Ajustes. En Ajustes, se puede configurar el acceso para no permitirlo nunca, permitirlo únicamente mientras se usa 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 forma adicional, a los usuarios se les otorga un control muy preciso del uso que hacen de la información sobre ubicación de los servicios del sistema. Este control incluye la posibilidad de desactivar la inclusión de información sobre la ubicación en la información que recopilan los servicios de diagnóstico y uso que utiliza 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 Spotlight, las condiciones del tráfico local y las ubicaciones visitadas frecuentemente para estimar los tiempos de viaje.

Acceso a datos personales

iOS evita que las apps puedan acceder sin permiso a la información personal del usuario. Además, en Ajustes, 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 física” en el iPhone 5s o posterior
- Cuentas de redes sociales tales como Twitter y Facebook
- Micrófono
- Cámara
- HomeKit
- HealthKit
- Compartir Bluetooth

Si el usuario inicia sesión en iCloud, las apps tienen permiso de acceso a iCloud Drive por omisión. Los usuarios pueden controlar el acceso de cada app a iCloud en Ajustes. Además, iOS proporciona restricciones que pueden impedir la transferencia de datos entre las apps y las cuentas que haya instalado MDM y aquellas que haya instalado el usuario.

Política de privacidad

La política de privacidad de Apple está disponible en línea en <https://www.apple.com/es/legal/privacy>.

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, el objetivo de iOS es cubrir las necesidades de cada empresa. La combinación de estos elementos permite a iOS contar con una seguridad líder en el sector sin que afecte a 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. Safari ofrece una navegación segura gracias a su compatibilidad con el Protocolo de estado de certificados en línea (OCSP), los certificados EV y los avisos de verificación de certificados. Mail utiliza certificados para su autenticación y encriptación compatibles con S/MIME que, a partir de iOS 8, permiten S/MIME por mensaje, así que los usuarios de S/MIME pueden optar por firmar y encriptar siempre los mensajes por omisión o controlar de forma selectiva cómo proteger cada mensaje. Además, 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 ofrece a los usuarios una sólida protección frente a virus, software malicioso y otros ataques que ponen en peligro la seguridad de otras plataformas. La finalidad del proceso de envío de apps a la App Store es proteger a los usuarios de estos riesgos mediante la revisión de cada app para iOS antes de que se ponga a la venta.

Para aprovechar al máximo las amplias funciones de seguridad integradas en iOS, animamos a las empresas a que revisen sus TI y políticas 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 experto equipo de seguridad con el fin de ofrecer soporte a 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 han lanzado al mercado. Además, el equipo de Apple proporciona herramientas de seguridad y formación, y supervisa activamente si hay informes de nuevos problemas y amenazas que ponen en riesgo la seguridad. Apple es miembro del Foro de equipos de seguridad y respuesta a incidentes (FIRST). Si desea obtener más información sobre cómo informar de incidencias a Apple y sobre la suscripción a las notificaciones de seguridad, visite apple.com/es/support/security.

Glosario

Actualización del firmware del dispositivo (DFU)	Modo en el que el código de la ROM de arranque de un dispositivo espera su recuperación mediante USB. Al estar en el modo DFU, la pantalla está en negro; sin embargo, tras conectarse a un ordenador en el que se ejecuta iTunes, se muestra el siguiente mensaje: "iTunes ha detectado un iPad en modo recuperación. Debe restaurar este iPad para poder usarlo en 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 y 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.
Cargador 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.
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.
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.
Correspondencia de ángulos del patrón de arrugas	Representación matemática de la dirección y la anchura de las arrugas extraída de una porción de una huella digital.
ECID	Identificador de 64 bits único en el procesador de cada dispositivo iOS. 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 pueden 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.
Grupo de acción de pruebas conjuntas (JTAG)	Herramienta estándar de depuración de hardware, que usan programadores y desarrolladores de circuitos.
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.
iBoot	Código que se carga mediante el LLB y que, a su vez, carga XNU como parte de la cadena de arranque seguro.
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 delicadas.
Módulo de seguridad de hardware (HSM)	Ordenador especializado en seguridad a prueba de manipulaciones que protege y gestiona 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 ítems del llavero.
Repositorio de claves	<p>Estructura de datos que se utiliza para almacenar un conjunto de claves de clase. Cada tipo (sistema, copia de seguridad, custodia o copia de seguridad de iCloud) tiene el mismo formato:</p> <ul style="list-style-type: none"> • Una cabecera contiene: <ul style="list-style-type: none"> – la versión (3 en iOS 5); – el tipo (sistema, copia de seguridad, custodia o copia de seguridad de iCloud); – el UUID del repositorio de claves; – un código HMAC si el repositorio de claves está firmado; – el método usado para la encapsulación de las claves de clase: vinculado al UUID o PBKDF2, junto con la sal y el recuento de iteraciones. • Una lista de claves de clase: <ul style="list-style-type: none"> – el UUID de las claves; – la clase (de qué clase de protección de datos de archivo o de llavero se trata); – tipo de encapsulación (solo clave derivada del UUID; clave derivada del UUID y clave derivada del código); – clave de clase encapsulada; – clave pública para clases asimétricas.
ROM de arranque	El primer código que ejecuta el procesador de un dispositivo al encenderse por primera vez. Como parte integral del procesador, ni Apple ni ningún atacante lo pueden alterar.
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 del procesador central A7 o posterior 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 cifrada y se fortalece con el UUID 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 cifrado con el UUID del dispositivo como la función pseudoaleatoria (PRF) para cada iteración.
XNU	Kernel ubicado en el corazón de los sistemas operativos iOS y OS X. 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.

© 2014 Apple Inc. Todos los derechos reservados. Apple, el logotipo de Apple, AirDrop, AirPlay, Bonjour, FaceTime, iBooks, iMessage, iPad, iPhone, iPod, iPod touch, iTunes, Llavero, Mac, OS X, Passbook, Safari, Siri, Spotlight y Xcode son marcas comerciales de Apple Inc., registradas en los EE. UU. y en otros países. Lightning y Touch ID son marcas comerciales de Apple Inc. iCloud y iTunes Store son marcas de servicio de Apple Inc., registradas en los EE. UU. y en otros países. App Store y iBooks Store son marcas de servicio de Apple Inc. iOS es una marca comercial o una marca comercial registrada de Cisco en los EE. UU. y en otros países y se usa bajo licencia. La marca denominativa y los logotipos de Bluetooth® son marcas comerciales registradas de Bluetooth SIG, Inc., y Apple dispone de licencia para usar dichas marcas. Java es una marca comercial registrada de Oracle y sus filiales. Otros nombres de productos y empresas mencionados en el presente documento pueden ser marcas comerciales de las respectivas empresas. Las especificaciones del producto están sujetas a cambios sin previo aviso. Octubre de 2014