Implantar el iPhone y el iPad
Certificados digitales

iOS admite certificados digitales, lo que ofrece a los usuarios de empresa un acceso seguro y sencillo a los servicios corporativos. Un certificado digital está formado por una clave pública, información sobre el usuario y la autoridad certificadora que lo emitió. Los certificados digitales son un medio de identificación que facilita la autenticación, la integridad de los datos y el cifrado.

En el iPhone y el iPad, los certificados se pueden usar de varias maneras. Firmar datos con un certificado digital ayuda a garantizar que esta información no pueda alterarse. Los certificados también pueden utilizarse para garantizar la identidad del autor o «firmante». Además, se pueden usar para cifrar perfiles de configuración y comunicaciones de red con el fin de aumentar la protección de información confidencial o privada.

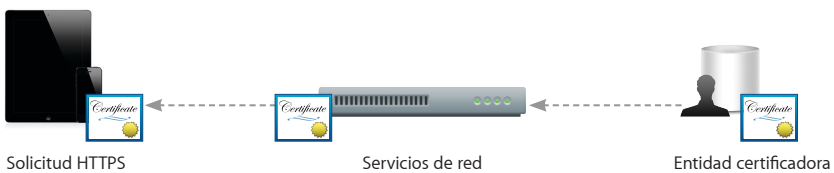
Usar certificados en iOS

Certificados digitales

Los certificados digitales sirven para autenticar de forma segura a usuarios de servicios corporativos sin necesidad de emplear nombres de usuario, contraseñas ni tokens por software. En iOS, la autenticación basada en certificados se usa para acceder a servidores de Exchange ActiveSync de Microsoft y a redes VPN y Wi-Fi.

Certificados de servidor

Los certificados digitales también se pueden usar para validar y cifrar comunicaciones de redes. Esto ofrece una comunicación segura, tanto con sitios web internos como externos. El navegador Safari puede comprobar la validez de un certificado digital X.509 y configurar una sesión segura con cifrado AES de hasta 256 bits. Así se verifica la legitimidad de la identidad del sitio y se garantiza la protección de la comunicación con el sitio web para ayudar a evitar la interceptación de datos personales o confidenciales.



Formatos de certificado e identidad compatibles:

- iOS admite los certificados X.509 con claves RSA.
- Se reconocen las extensiones de archivo .cer, .crt, .der, .p12, y .pfx.

Certificados raíz

De serie, iOS incluye diversos certificados raíz preinstalados. Para consultar una lista de estos certificados, lee el artículo de Soporte de Apple que encontrarás en http://support.apple.com/kb/HT4415?viewlocale=es_ES. Si usas un certificado raíz que no está preinstalado, como un certificado raíz autofirmado creado por tu empresa, puedes distribuirlo mediante uno de los métodos enumerados en la sección «Distribuir e instalar certificados» de este documento.

Distribuir e instalar certificados

Distribuir certificados al iPhone y al iPad es fácil. Cuando recibe un certificado, el usuario solo tiene que tocarlo para ver su contenido y volver a tocar para añadir el certificado al dispositivo. Al instalar un certificado de identidad, se solicita al usuario que introduzca la contraseña que lo protege. Si no se puede verificar la autenticidad de un certificado, los usuarios recibirán un aviso antes de que se añada a su dispositivo.

Instalar certificados mediante perfiles de configuración

Si se usan perfiles de configuración para distribuir los ajustes de los servicios corporativos, como Exchange, VPN o Wi-Fi, los certificados se pueden añadir al perfil con el fin de optimizar la implantación.

Instalar certificados mediante Mail o Safari

Si se envía un certificado en un correo electrónico, se mostrará como un adjunto. Se puede usar Safari para descargar certificados desde una página web. Puedes alojar un certificado en un sitio web seguro y facilitar a los usuarios la URL desde la que pueden descargar el certificado en sus dispositivos.

Instalación mediante el protocolo SCEP (Simple Certificate Enrollment Protocol)

SCEP está diseñado para ofrecer un acceso simplificado para administrar la distribución de certificados en implantaciones a gran escala. Esto permite la inscripción inalámbrica de certificados digitales en el iPhone y el iPad. Estos certificados se pueden utilizar para la autenticación del acceso a servicios corporativos, y también para la inscripción en un servidor de gestión de dispositivos móviles.

Para obtener más información sobre el protocolo SCEP y la inscripción inalámbrica, consulta los recursos disponibles en www.apple.com/es/iphone/business/resources.

Revocación y eliminación de certificados

Para eliminar un certificado ya instalado manualmente, selecciona Ajustes > General > Perfiles. Si eliminas un certificado necesario para acceder a una cuenta o red, el dispositivo no podrá volver a conectarse a esos servicios.

Para eliminar certificados de forma inalámbrica se puede usar un servidor de gestión de dispositivos móviles. Este servidor puede ver todos los certificados de un dispositivo y eliminar los que tenga instalados.

Además, se admite el protocolo OCSP (Online Certificate Status Protocol), que sirve para comprobar el estado de los certificados. Cuando se usa un certificado que emplea OCSP, iOS lo valida para comprobar que no haya sido revocado antes de completar la tarea solicitada.

 Septiembre de 2012