Deploying iPhone and iPad
Digital Certificates

Supported certificate and identity formats:

- iOS supports X.509 certificates with RSA keys.
- The file extensions .cer, .crt, .der, .p12, and .pfx are recognized.

Root certificates

Out of the box, iOS includes a number of preinstalled root certificates. To view a list of the preinstalled system roots, see the Apple Support article at http://support.apple.com/kb/HT4415. If you are using a root certificate that is not preinstalled, such as a self-signed root certificate created by your company, you can distribute it using one of the methods listed in the "Distributing and Installing Certificates" section of this document.

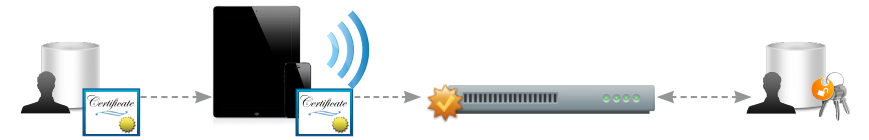
iOS supports digital certificates, giving business users secure, streamlined access to corporate services. A digital certificate is composed of a public key, information about the user, and the certificate authority that issued the certificate. Digital certificates are a form of identification that enables streamlined authentication, data integrity, and encryption.

On iPhone and iPad, certificates can be used in a variety of ways. Signing data with a digital certificate helps to ensure that information cannot be altered. Certificates can also be used to guarantee the identity of the author or "signer." Additionally, they can be used to encrypt Configuration Profiles and network communications to further protect confidential or private information.

Using Certificates in iOS

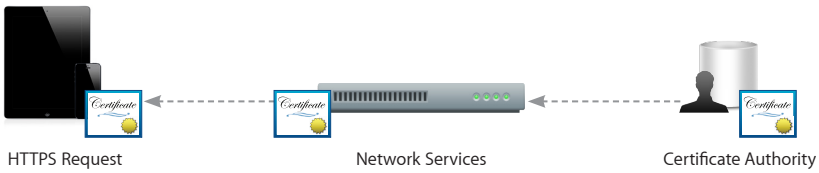
Digital certificates

Digital certificates can be used to securely authenticate users to corporate services without the need for user names, passwords, or soft tokens. In iOS, certificate-based authentication is supported for access to Microsoft Exchange ActiveSync, VPN, and Wi-Fi networks.



Server certificates

Digital certificates can also be used to validate and encrypt network communications. This provides secure communication to both internal and external websites. The Safari browser can check the validity of an X.509 digital certificate and set up a secure session with up to 256-bit AES encryption. This verifies that the site's identity is legitimate and that communication with the website is protected to help prevent interception of personal or confidential data.



Distributing and Installing Certificates

Distributing certificates to iPhone and iPad is simple. When a certificate is received, users simply tap to review the contents, then tap to add the certificate to their device. When an identity certificate is installed, users are prompted for the passphrase that protects it. If a certificate's authenticity cannot be verified, users will be presented with a warning before it is added to their device.

Installing certificates via Configuration Profiles

If Configuration Profiles are being used to distribute settings for corporate services such as Exchange, VPN, or Wi-Fi, certificates can be added to the profile to streamline deployment.

Installing certificates via Mail or Safari

If a certificate is sent in an email, it will appear as an attachment. Safari can be used to download certificates from a web page. You can host a certificate on a secured website and provide users with the URL where they can download the certificate onto their devices.

Installation via the Simple Certificate Enrollment Protocol (SCEP)

SCEP is designed to provide a simplified process to handle certificate distribution for large-scale deployments. This enables Over-the-Air Enrollment of digital certificates on iPhone and iPad that can then be used for authentication to corporate services, as well as enrollment with a Mobile Device Management server.

For more information on SCEP and Over-the-Air Enrollment, visit www.apple.com/iphone/business/resources.

Certificate removal and revocation

To manually remove a certificate that has been installed, choose Settings > General > Profiles. If you remove a certificate that is required for accessing an account or network, the device will no longer be able to connect to those services.

To remove certificates over the air, a Mobile Device Management server can be used. This server can view all certificates on a device and remove ones it has installed.

Additionally, the Online Certificate Status Protocol (OCSP) is supported to check the status of certificates. When an OCSP-enabled certificate is used, iOS validates it to make sure that it has not been revoked before completing the requested task.