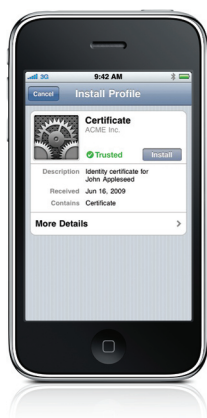




iPhone in Business

Digital Certificates



Supported certificate and identity formats:

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

Root certificates

Out of the box, iPhone 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/HT2185>. 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 to iPhone using one of the methods listed in the "Distributing and Installing Certificates" section of this document.

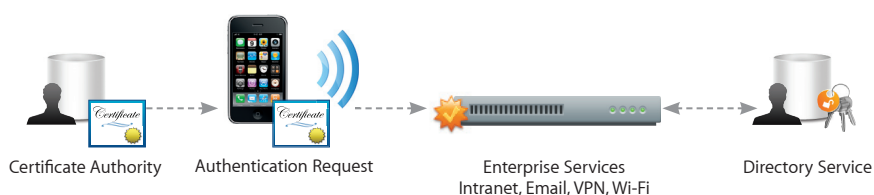
iPhone supports digital certificates, giving business users secure, streamlined access to corporate services. A digital certificate is composed of a public and private key pair, along with other information about you and the certificate authority that issued the certificate. Digital certificates are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

Certificates can be used to sign and encrypt many types of data. Data signed with a digital certificate helps to ensure that it has not been changed or altered, and can also be used to guarantee the identity of the author or "signer." Additionally, certificates can be used to encrypt configuration profiles and network communications to help further protect confidential or private information.

Using Certificates on iPhone

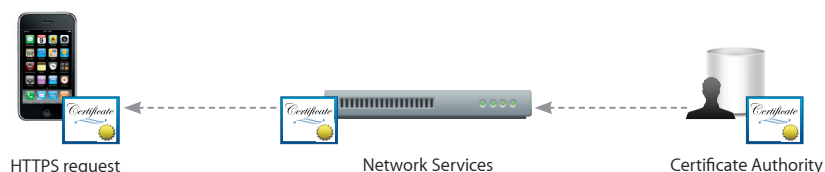
Identity certificates

Digital certificates can be used to securely authenticate users to corporate services without the need for user names, passwords or even tokens. On iPhone, certificate-based authentication is supported for access to Microsoft Exchange ActiveSync, Cisco IPsec VPN, and WPA2 Enterprise Wi-Fi networks.



Server certificates

Digital certificates can also be used to validate and encrypt network communications. This provides secure communication to both internal websites and websites on the public Internet. The Safari browser can check the validity of the X.509 digital certificate being presented and set up the secure session with 128-bit SSL encryption. This verifies that the site's identity is legitimate and that your communication with the website is protected to help prevent interception of personal or confidential data.



Distributing and Installing Certificates

Distributing certificates to iPhone is simple. Whenever you receive a certificate, it can be imported into your keychain for later use. When an identity certificate is installed, the user is prompted for the passphrase that protects it. If a certificate's authenticity cannot be verified, you will be presented with a warning before it is added to your keychain. Certificates can be distributed to iPhone in four ways.

Installing certificates via a configuration profile

If you are using configuration profiles to distribute settings to corporate services such as Exchange, VPN, or Wi-Fi, certificates can be added to the profile to streamline deployment. If you're using multiple configuration profiles, make sure certificates aren't duplicated. You cannot install multiple copies of the same certificate.

1. Under the Credentials tab in the iPhone Configuration Utility, click Configure.
2. In the file dialog that appears, select a PKCS#1 or PKCS#12 file, and then click Open.

To add multiple credentials to the configuration profile, click the Add (+) button.

Mac OS X

If the certificate or identity that you want to install is in your keychain, use Keychain Access to export the credential in .p12 format before creating your profile.

Windows

If the credential is not available in your personal certificate store, you must add it before creating your profile, and the private key must be marked as exportable, which is one of the steps offered by the certificate import wizard. Note that adding root certificates requires administrative access to the computer, and the certificate must be added to the personal store.

Installing certificates via Mail

If a certificate is sent in an email, it will appear as an attachment. The user simply taps on the attachment to review and taps install to add the certificate to his or her device.

Installing certificates via Safari

Safari can be used to download certificates from a web page. 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 an Internet draft in the Internet Engineering Task Force (IETF) that is designed to provide a simplified way of handling certificate distribution for large-scale deployments. This enables over-the-air distribution of identity certificates to iPhone that can be used for authentication to corporate services.

Certificate removal and revocation

To 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, your device cannot connect to those services.

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