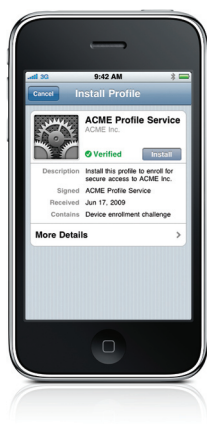




iPhone in Business

Over-the-Air Enrollment and Configuration



iPhone and SCEP

iPhone supports the Simple Certificate Enrollment Protocol (SCEP). SCEP is an internet draft in the IETF, and is designed to provide a simplified way of handling certificate distribution for large-scale deployments. This enables over-the-air enrollment of identity certificates to iPhone that can be used for authentication to corporate services.

iPhone supports over-the-air enrollment and configuration, providing an automated way to configure devices securely within the enterprise. Enrollment refers to the process of authenticating a device and user for the purposes of automated certificate distribution. While over-the-air enrollment facilitates the general deployment of device certificates within your company's public key infrastructure (PKI), it also can facilitate the distribution of signed and encrypted configuration profiles. The combined process of certificate enrollment and device configuration provides IT with assurance that only trusted users are accessing corporate services, and that their devices are properly configured to comply with established policies. And because configuration profiles can be both encrypted and locked, the settings cannot be removed, altered, or shared with others.

Administrators can prompt the user to begin the process of enrollment by providing a URL via email or SMS notification. By agreeing to the profile installation, the users' device is automatically enrolled and configured in a single session.

Process Overview

The process of over-the-air enrollment and configuration involves three phases that when combined, in an automated workflow, provide a secure way to provision devices within the enterprise. These phases include:

1. User Authentication

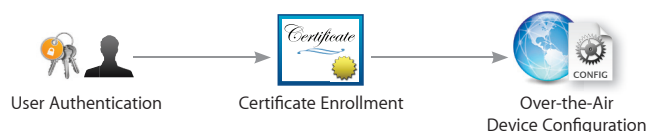
User authentication ensures that incoming enrollment requests are from authorized users and that the user's device information is captured prior to proceeding with certificate enrollment.

2. Certificate Enrollment

After the user is authenticated, iPhone generates a certificate enrollment request using the SCEP protocol. This SCEP enrollment request talks directly to the enterprise Certificate Authority (CA), and enables iPhone to receive the identity certificate from the CA in response.

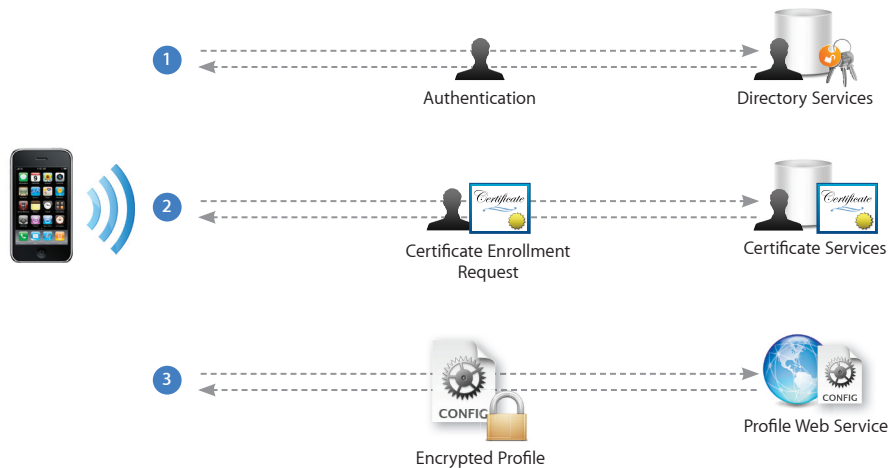
3. Device Configuration

Once an identity certificate is installed, iPhone is able to receive an encrypted configuration profile over-the-air. This encrypted configuration profile can only be installed on the device it was intended for and can contain settings for iPhone to connect to corporate services (Exchange, VPN, Wi-Fi, etc.)



User Scenario

The following example shows how iPhone connects to a typical over-the-air enrollment and configuration deployment.



- 1 The user enters the URL of the profile service in Safari on iPhone (or taps a URL sent by the administrator via SMS), and is presented a login webpage. The user enters their username and password. The user is authenticated using either basic HTTP authentication or via existing directory services.
- 2 Once the user is authenticated, an enrollment profile is sent to the user. The user is prompted to install the profile. Once the initial enrollment profile is installed, iPhone responds back to the certificate authority with information necessary to deliver an identity certificate to the device.
- 3 That identity certificate enables the device to receive device settings via an encrypted configuration profile. This exchange is automated. No additional interaction from the user is required.

Infrastructure Setup

To implement this process you will need to create an infrastructure which can support the authentication, enrollment, and profile delivery process. The deployment and integration of three primary enterprise services is involved.

Directory Services

User authentication can be as simple as basic HTTP authentication, or you can integrate with your existing directory services. Regardless of the services used, you will need to provide a web-based authentication method for your users to request enrollment.

Certificate Services

The process of enrollment requires deployment of standard x.509 identity certificates to iPhone users. You'll need a CA (certificate authority) to issue the device credentials using the Simple Certificate Enrollment Protocol (SCEP). Cisco IOS and Microsoft Server 2003, with the add-on for certificate services both support SCEP. There are also a number of hosted PKI services that support SCEP, such as Verisign, Entrust, and RSA.

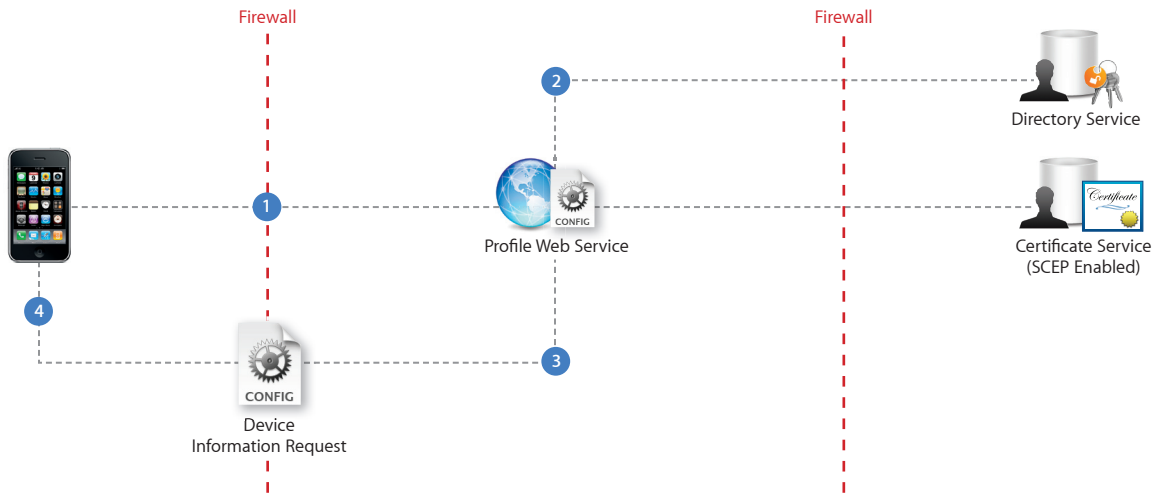
Profile Services

To implement this process you will need to develop a profile service, which is an HTTP-based service that manages iPhone connections throughout the process, generates configuration profiles for the user, and verifies user credentials along the way. There are a few key functions that the profile service needs to provide:

- Host a user-accessible website to support the HTTPS session
- Authenticate incoming user requests using a web-based authentication method (basic, or integrated with directory services)
- Generate the necessary configuration profiles (XML format) depending on the phase of the process
- Sign and encrypt configuration profiles using public key cryptography
- Track the user through the steps in the process (via timestamp and logging methods)
- Manage connections to the certificate authority or directory services

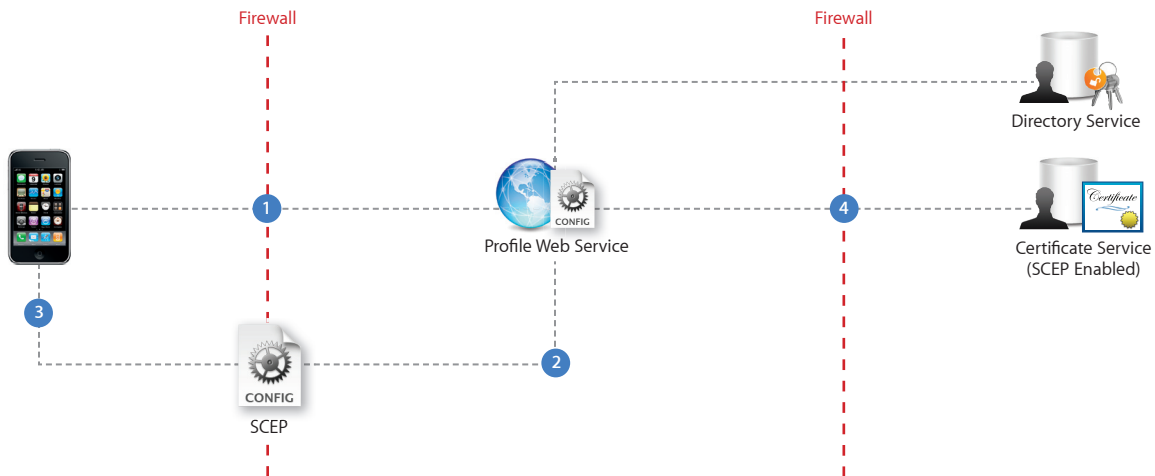
The following three diagrams describe the individual steps in each phase that need to be in place for a typical over-the-air enrollment and configuration implementation.

Phase 1: User Authentication



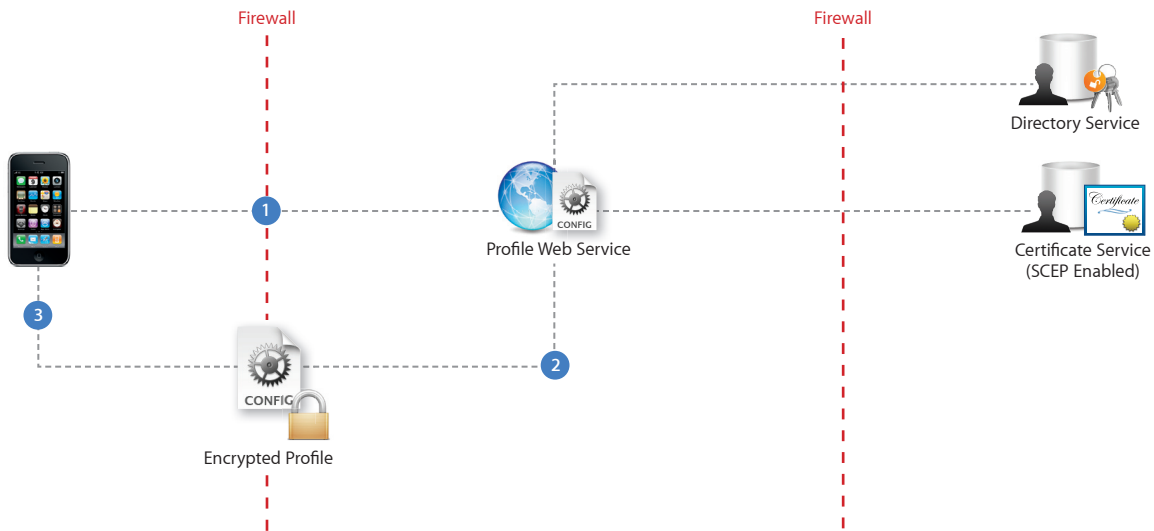
- 1 The user enters the URL of the profile service in Safari on iPhone (or taps a URL sent via SMS), and is presented a login webpage. The user enters their username and password.
- 2 The user is authenticated using either basic HTTP authentication or via existing directory services.
- 3 Once the user is authenticated, a configuration profile is sent to the user. This profile includes a request for device attributes including the device identifier (iPhone or iPod Touch), OS version, Device ID, IMEI, and ICCID. For a sample configuration profile for this phase, see "Server Response" on page 81 of the Enterprise Deployment Guide.
- 4 The user is prompted to install the profile.

Phase 2: Certificate Enrollment



- 1 Once the configuration profile from Phase 1 is installed, the device automatically responds to the server. The response from the device includes device attributes and a pre-shared key (challenge). The challenge can be used to verify the identity of the user through the next phase of the process. The response is signed using the device's built-in identity (Apple issued certificate) and sent to the server using HTTP Post.
- 2 Once the profile service receives the device response, a second configuration profile with the SCEP payload is delivered to the device. For a sample configuration profile for this phase, see "Server Response With SCEP Specifications" on page 82 of the Enterprise Deployment Guide.
- 3 The profile is installed automatically, no user intervention required. The SCEP payload contains instructions for the device to generate a certificate signing request and get a certificate using SCEP.
- 4 Once the request is verified, the CA then issues the certificate for the device.

Phase 3: Device Configuration



- 1 Once the device certificate is received, the device generates a response back to the profile service which is signed with the new certificate (again, via HTTP post). The response includes device attributes (product identifier, OS version, Device ID, IMEI, and ICCID). This information provides a confirmation to the server, at the time of request, and can be used to ensure devices are up to date with the latest OS version before delivering a configuration profile.
- 2 The profile service then responds with an encrypted .mobileconfig file. This configuration profile can contain policies, settings, credentials, or additional SCEP requests.
- 3 The profile is received by the device and installed automatically (no user intervention is required).