# Client Cert Use Cases

## Client Certificates: Use Cases

### S/MIME E-mail

Before Bob sends an S/MIME e-mail message to Mary, he signs the message with his private key and encrypts the message with Mary's public key. Mary, upon receiving the message, verifies the signature using Bob's public key and decrypts the message using her private key. In this way, the message is mutually authenticated, integrity protected, and confidential.

Both Bob and Mary's private decryption keys are escrowed by their respective organizations (or departments). If either Bob or Mary were to lose their private decryption keys, the institution (or department) could restore the key so that archived e-mail could be decrypted and read. Doing so would automatically revoke the key, however, which would require the issuance of a new decryption key.

Since Bob and Mary's e-mail is encrypted, it is unreadable by third parties. However, because the encryption keys are escrowed, the organization (or department) would be required to surrender unencrypted e-mail if subpoenaed by a Court. Without escrow enabled, only Bob and Mary themselves would be subject to subpoena (since only they would hold the private decryption keys).

### Certificate Enrollment on the iPhone

A system administrator prompts Alice, an iPhone user, to begin the process of certificate enrollment by providing a URL via SMS notification. Alice clicks the link in the SMS message to automatically launch the Safari browser on her iPhone. Before proceeding with certificate enrollment, the server prompts Alice to authenticate with her institutional username and password. She does so, after which the enrollment process begins automatically.

The server responds to Alice's successful authentication with a request for device attributes, including the MAC address and IMEI serial number of the iPhone. Once Alice clicks "okay," the iPhone and the server automatically begin a series of message exchanges (via a protocol called Simple Certificate Enrollment Protocol, or SCEP) that culminate in an enterprise X.509 certificate being downloaded to Alice's iPhone over the air.

If Alice chooses to accept the X.509 certificate, a configuration profile is downloaded to her iPhone as well. The configuration profile may enforce institutional policy with respect to the X.509 certificate, such as the requirement for a PIN to protect against a lost or stolen iPhone. It is up to Alice to decide whether or not to keep the X.509 certificate subject to policy.

Once the X.509 certificate is installed on the iPhone, Alice is able to connect to the campus VPN (and other services) securely and transparently, without prompting or input. When the installed X.509 certificate expires or is revoked, Alice's iPhone automatically repeats the above process, without Alice having to initiate the procedure.