InCommon Personal Certificate Provisioning and Application Setup Tool

January 3, 2012

Introduction

The major reason that PKI technology and end user personal certificates have not been more heavily leveraged on our campuses is the complexity of the end user workstation set up process. Once certificates are installed and the user's applications are properly configured, digital certificates enhance security and are more convenient and easier to use than other authentication mechanisms. A few schools have solved this configuration complexity problem by developing automated solutions for workstation certificate life-cycle management and PKI-enabled application configuration. The purpose of this document is to combine the best features of the existing tools with the results of our discussions and more clearly define what is needed in a central InCommon supported certificate management. The expectation is that the tool will either be developed and maintained by the community or outsourced to a commercial provider.

The overall goal for the proposed tool is to make digital certificates a common choice for a set of campus-based and inter-institutional standard assurance applications including (a) web authentication to the campus SSO environment (typically Shibboleth), (b) wireless LAN authentication, (c) VPN authentication, (d) signed electronic mail, (e) eduroam, and, to a lesser extent, other PKI-enabled applications that leverage the native operating system certificate store such as document signing. With the exception of electronic mail and eduroam users, digital certificate use is focused on expanding campus-level security by enhancing the initial user authentication process. For example, digital certificates are not vulnerable to phishing attacks. Digital certificates easily integrate into campus infrastructure and typically complement and enhance existing single sign-on solutions as opposed to replacing them.

The InCommon Workstation Setup Tool is designed to be modular, easily extensible, and is expected to perform automated tasks such as obtaining user and intermediate certificates, installing them in appropriate workstation key store(s), handling certificate life-cycle management for the end user, and configuring appropriate workstation applications to use the installed certificates. Important workstation security configuration issues will also be addressed by the tool.

The tool is one component of an overall program to support the adoption of InCommon personal digital certificates by campuses. The program will also need to include documentation and templates for campus system administrators on how to support certificates with the campus infrastructure. The functionality described below assumes that Comodo will be able to deliver on their sub-5 second certificate issuance commitment using a simple synchronous transaction.

Client-Server System Outline

As depicted in Figure 1, the tool can be implemented using a simple client-server configuration with as many of the common tasks as practical managed on a central campus server. The more specialized code for each supported operating system is bundled into an application that is installed and runs on individual user workstations.

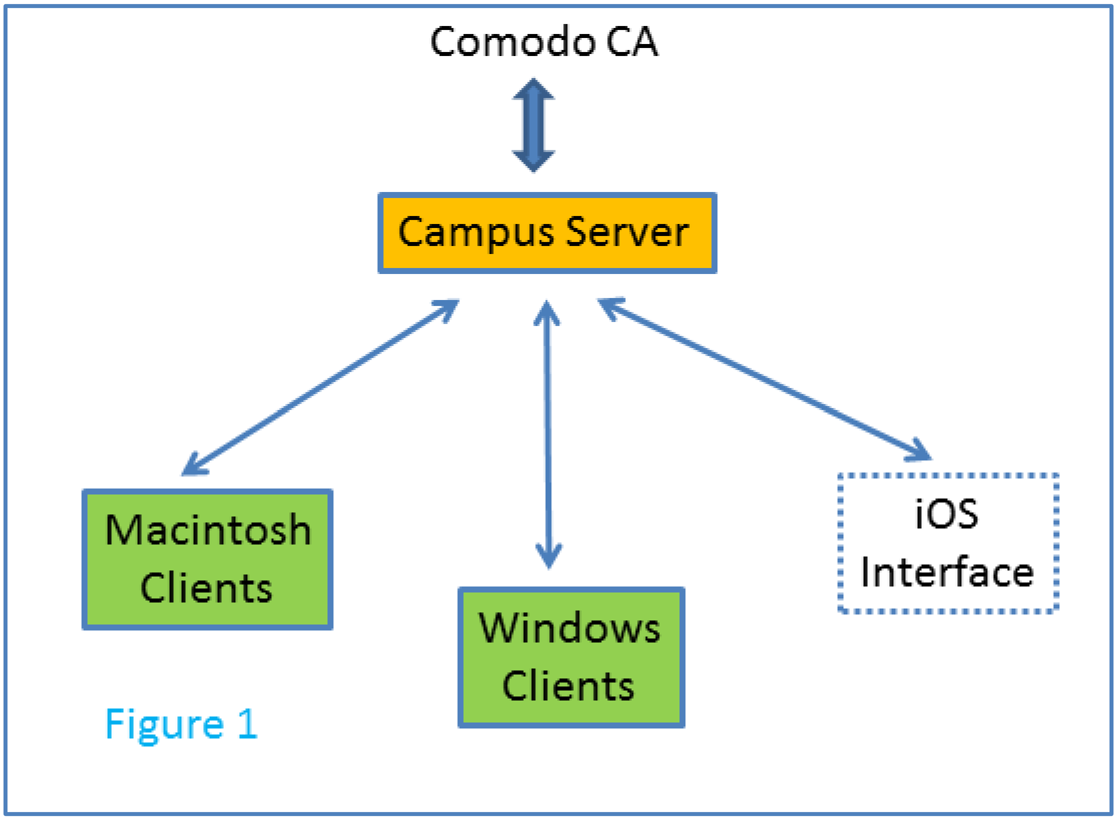

Figure 1

Macintosh and Windows client software process outline:

a. All communication with the server is assumed to be over SSL with the client verifying the server's certificate before proceeding.
b. Each invocation of the client software starts with the client communicating with the server to determine the supported campus client version number. Information is provided back to the user when an upgrade is needed. The client tests for minimum legal version numbers and refuse to operate, as needed, when an upgrade is required by the campus.
c. The client checks to determine if a usable certificate is already installed on the workstation. If no such certificate exists, the user is prompted to determine if they would like to obtain a certificate.
d. The client collects authentication credentials from user when a new certificate is needed. The exact number of authentication credentials requested by the client and the names of the fields displayed to the user are based configuration data stored on the server. Example campus usage might include User ID, Password, Date of Birth, etc. Up to five

parameters are to be accepted. At least one primary password and campus unique user id (EPPN) are required.

e. The client software also collects workstation attribute information such as the wireless and wired interface MAC Ethernet addresses and a hostname (from the OS or a user prompt). Use an extensible format to enable simple future extension of this data.
f. The client sends the authentication, MAC address, and other information to the server as part of any request for a new certificate. Once a request is submitted, the client waits for the server's reply containing either an error message or a PKCS12 holding the user's certificate and private key. The PKCS12 delivered by the server is encrypted with the user's password.
g. The certificate and private key are installed into the operating system's native store. If possible, mark the private key as not exportable (this is possible on Windows).
h. Optionally, install the certificate and private key into the Mozilla store if Firefox is present on the device. Ensure that the Firefox store is password protected before proceeding.
i. Install any needed intermediate certificates.
j. Provide optional functionality to run each time the user logs into their workstation to test to see if their certificate is about to expire. If it will expire in the next 30 days, prompt the user to obtain a replacement certificate.
k. Optionally download and apply the site's wireless LAN settings.
l. Optionally download and apply the site's required password protected screen saver settings.
m. Optionally download and apply the site's requirements for workstation user login.
n. Optionally download and apply the site's required email client settings for S/MIME.
o. On Windows, optionally download and apply the site's Windows firewall configuration script.
p. Each of the above workstation configuration steps must be designed to be run as often as desired by the end user. Each time a step is run, it should ensure that the proper configuration is set on the user's workstation.

Apple iOS web service process outline:

a. Collect authentication credentials from user. The exact number of authentication attributes requested and the names of the fields as presented to the user are based configuration data stored on the server. Example campus usage might include User ID, Password, Date of Birth, etc. Up to five parameters are to be accepted. At least one primary password and campus unique user id (EPPN) are required.
b. Download an iOS security profile containing (a) the user's certificate and private key, (b) the site's wireless LAN configuration data, (c) a password policy that requires device authentication and device wipe on failed attempts, and optionally (d) the site's VPN settings. These requirements ensure that if the user removes the device password protection that they also delete their private key.

Central Server process outline:

a. Provide services to client software over a simple (perhaps REST-style) interface. The design should not require the server to store any state across requests.
b. Accept and respond to a request for supported client versions. Both the current and the minimum legal campus version must be supplied in the response.
c. Accept and respond to a request for a new personal certificate

    a. Validate the authentication credentials supplied by the end user. This is done via calling an authentication service provided by the host campus and accepting back a yes/no answer.
    b. Generate a key pair for the user, obtain a certificate from Comodo, package the certificate and private key into a PKCS12 object that is encrypted with the user's password.
    c. Send the PKCS12 back to the client software.
    d. Optionally call a host campus service providing the user's certificate, the user's hostname, the MAC addresses from the user's workstation, the user's EPPN, and the IP address of the requesting host. This option enables campuses to simplify network registration tasks.
    e. Log the information listed in item (d) above along with the current date and time.

d. Accept and respond to requests for intermediate certificates.
e. Accept and respond to requests for site security requirements. This data is used by the client to determine which features are optional for the end user and which are mandatory per site policy.
f. Accept and respond to requests for the site's wireless LAN configuration.
g. Accept and respond to requests for the site's password protected screen saver policy.
h. Accept and respond to requests for the site's workstation login requirements
i. Accept and respond to requests for the site's S/MIME email client configuration.
j. Accept and respond to requests for the site's workstation firewall configuration.

Additional information on some of the more common certificate-enabled applications and their requirements are discussed in the Client Certificate Roadmap document.

Additional System Opportunities

Many opportunities exist for future enhancements to the tools including:

a. Safe deletion of expired certificates.
b. Additional workstation security settings and configuration management.
c. Assistance with software installation and/or configuration for 2-factor authentication devices supported by InCommon.
d. …