Client Certificate Deployment Roadmap

This document is a work in progress, intended to evolve over time. Experience and suggestions from the community are welcomed and desired.

See also the following documents attached to this page:

- InCommon survey on Campus Use of 2-Factor Authentication
- InCommon Personal Certificate Provisioning and Application Setup Tool

Please direct comments/feedback to Paul Caskey <pcaskey AT internet2.edu>

Introduction

The ability to *mint* digital certificates for your users is really just one small component of the overall work involved in a successful campus-wide PKI deployment. Many campus PKI projects have been less than successful by not focusing enough on the whole product and the usability of the applications they support with certificates. If deployed properly, digital certificates can build a more secure environment while also being more convenient for users than traditional password-based systems. Some examples of campus-based certificate-enabled applications, listed below in a reasonable campus deployment order, include:

- **VPN Authentication**
  Like web authentication, once a user has a certificate installed on their workstation, it can typically be leveraged easily by most IPsec and SSL VPN systems. The use of certificates for VPN authentication eliminates the need for users to type their password and often removes the need to maintain an additional password database. Simply clicking on the connect button provides a secure VPN path.
- **Wireless Authentication**
  The use of certificates and EAP-TLS and certificates for authentication to the campus wireless networks improves security and is a significant ease of use enhancement for end users. From a user's perspective, when their device is within range of a campus Access Point, it securely connects in the background. No captive portal, entering passwords, or other such inconvenient mechanisms. Certificate-based wireless authentication also removes significant risk from rogue access points being used to capture user passwords. Migrating to EAP-TLS for wireless authentication also prepares a campus for simple configuration into eduRoam. You may also wish to pursue the use of certificates to authenticate users to the campus wired network.
- **Web Authentication**
  Most web servers and browsers make certificate-based authentication easy to implement and use. A typical campus implementation might prefer the use of certificates over passwords for authentication to the central campus Web SSO system. Application owners should always consider if part of their user community (e.g., guests) may not have certificates. The use of certificates eliminates the risk associated with phishing attacks. While web authentication to local campus systems can work seamlessly because the Subject DN or other content can be understood, web authentication to external systems is more problematic. First, the DN may expose more information than necessary (a privacy concern), or, second, it might not provide what is actually needed by the external RP. InC-PKI might develop and demonstrate use of a DN containing only an abstract identifier, and a Subject_info_access (SIA) field containing a pointer(s) to a campus IdMS "Backend Attribute Exchange" (BAE) server.
- **Signed Electronic Mail**
  A campus certificate infrastructure makes it possible to promote S/MIME-based digital signing of electronic mail messages. Many modern email clients support signed email messages as do some webmail applications (e.g., Outlook Web Access and Stalker). Highlight: official announcements, mailing list issues, client interoperability, webmail, client configuration, etc.
- **Encrypted Electronic Mail**
  Many email clients support the ability to use digital certificates to encrypt messages. While this facility can be useful for the short term transport of sensitive data, the use of encryption also comes with a set of issues that should be carefully considered before deployment.
- **Digital Signatures**
  Signing other documents, such as in the Microsoft Office Suite and Adobe products. This could include protocols for being able to verify signatures after the signing certificate expires. In particular, use of DS for maintaining archival versions of important documents may require this. Another use case might be signed web pages to ensure readers that the content was produced by the supposed source. Browsers that can accommodate "extensions" (Firefox, Safari) could make use of this capability.
- **Globus and Grid Computing**
  Grids worldwide rely on X.509 client certificates for authentication of users and processes. Grid access control is based on lists (ACLs) of X.509 subject DNs (i.e., identity-based access control). Of particular note is the heavy use of X.509 proxy certificates within the grid community. A proxy certificate is derived from and signed by an ordinary X.509 end-entity credential (or another proxy credential). Note: InCommon Standard Assurance Client Certificates are designed to work well with Globus but are not issued at an IGTF level of assurance that meets the needs of grids such as TeraGrid or Open Science Grid.

All certificate-based applications depend on the user's certificates and their associated private keys being pre-installed in appropriate location(s) such that they are accessible to applications as needed but still under the control of the user. Some PKI-enabled applications require further setup on the user's device and others, such as VPN clients, often require workstation firewall tuning for successful operation. The level of user acceptance, and thus the success of the overall project, often depends on how easy it is for users to have their certificates installed in all of the needed locations on their workstations and mobile devices, have their applications preconfigured for certificate use, and how well users are warned when expiring certificates need to be replaced.

Service Considerations

The first consideration for making certificate-enabled services function transparently for users is a friendly mechanism to have their certificate and private key installed in all of the needed location(s) on their workstations and mobile devices. This mechanism would typically be done with the certificates installed in a non-exportable way. Basic workstation security settings such as a password protected screen savers can also be verified as part of the installation process. Certificate store requirements for the common applications listed above are summarized in the table below:

Service Name	Platform	Certificate Store Requirements
Web Authentication	Windows	Windows OS store for IE, Mozilla Store for Firefox, others
	Macintosh	Apple OS store (keychain) for Safari, Mozilla store for firefox, others

VPN Authentication	Windows	Windows OS certificate store is typical
	Macintosh	Apple OS certificate store (keychain) is typical
Wireless Authentication	Windows	Windows OS certificate store
	Macintosh	Apple OS certificate store (keychain)
Signed EMail		Varies by email client. Some clients support the native operating system certificate store and others do not.
Digital Signatures		Varies by email client. Some clients support the native operating system certificate store and others do not.
Encrypted Email		Varies by email client. Some clients support the native operating system certificate store and others do not.
Globus	All	Since proxy certificates are typically short-lived, a proxy credential is stored in the file system at a well-known location

Also important to the success of a campus PKI deployment are tools that effectively warn the user when their certificate is about to expire. This is best done directly on the workstation with the expiring certificate as opposed to some email-based mechanism that requires a user to keep track of which certificate is installed on a particular system.

InCommon PKI Subcommittee Standard Assurance Certificate Project Roadmap

1. **Certificate Availibility**
   Work within InCommon and with Comodo to make certificates available. This process involves (a) depeloping the appropriate CPS and having it approved by InCommon and Comodo, (b) creating a certificate profile that works well with known campus PKI-enabled applications, and (c) working with Comodo to make these certificates available via their web site.
2. **Certificate Enabled Applications**
   Document typical campus PKI-enabled applications and services including information on how these applications are typically enabled, configurations, and a summary of items to consider before deploying the application. This work will also highlight the issues associated with encryption and especially encrypted email.
3. **Mobile Devices (e.g., iPhone and Android)**
   Provide information and guidance on the use of certificates on mobile devices such as iPhones and Android devices. This includes advice on how to enable security profiles that enforce device PINs to protect the certificate and its use. Mobile devices are lost more frequently than workstations and laptops.
4. **Comodo Client Certificates API**
   Evaluate the suitability of the Comodo API (as opposed to web interface) for the rapid issuance of certificates to large numbers of users. Recommend changes if/as needed. *Evaluarion and testing revealed the need for two Comodo enhancements: (a) a sub-5-second response for client certs in order to provide real-time response for end-user certificate provisioning and (b) overall capacity enhancements to enable the Comodo CA to better deal with a large number of certificates issued on a single day, such as on a first-year move-in day. Comodo is working to add both of these enhancements,*
5. **Certificate Installation Automation**
   Evaluate tools that automate the installation of certificates on user workstations and manage the setup of certificate enabled applications (e.g., wireless profiles, firewall for VPN, etc). These tools should also facilitate certificate management and renewal. *Developing Certificate Installation Automation Tools is the path the the working group has chosen to follow to help facilitate the practical use of Client Certiticates on campus.*
6. **SCEP**
   A useful tool might be the Simple Certificate Enrollment Protocol (SCEP), an X.509 certificate enrollment protocol that simplifies the distribution of certificates. Determine what it can be used for.
7. **Shibboleth-enabled Access**
   Work with Comodo to facilitate the creation of a Shibboleth-based interface for the issuance of end user certificates.

Some References

Reference Page

File	Modified
PDF File InCommon-2-Factor-AuthN-Survey.pdf InCommon 2-Factor Authentication Survey	Nov 16, 2011 by Jim Jokl (virginia.edu)
PDF File InCommonCertToolv2.pdf	Jan 04, 2012 by Jim Jokl (virginia.edu)

Download All