The Global Identity and Access Management Infrastructure and Your Campus Network

Network Device Provisioning

Spring Internet2 Meeting
April 23, 2013

Jim Jokl
University of Virginia
The Problem Set

- Enable the use of strong authentication
  - Passwords are painful and phishing is easy
  - Enhanced authentication must be simple for end-users to use and add real security

- Automation for on-boarding of devices on to the campus network
  - Configuration for campus network
  - Device MAC address registration
  - Security settings
Strong Authentication via Digital Certificates

- A binding between a name and a cryptographic key pair
- The binding is performed by a Certification Authority that is trusted by everyone
- Some common uses
  - Identifying web sites and supporting SSL encryption
  - Digital signatures for software distribution
  - Identifying people (and devices) for authentication
Personal Certificates

- **Common Uses for Standard Assurance Certificates**
  - Web authentication
  - VPN authentication
  - Wireless authentication (EAP-TLS)
  - S/MIME for signed (and encrypted) email
  - Digital signatures
  - Globus / Grid

- **InCommon Client Certificate Site**
  - [https://www.incommon.org/cert/clientcerts.html](https://www.incommon.org/cert/clientcerts.html)
Personal Certificates

• At UVa
  • Have used personal certificates for many years
    • Everyone has a certificate (or two)
  • Wireless, VPN, web authentication (to our SSO), etc
    • Generally more convenient to use and much more secure than passwords
  • Key to success: easy certificate lifecycle management
    • We use a Certificate Provisioning Tool

On your computer?
Log in with your UVa Digital Certificate
(What's this? | Get one now!)
Less typing. More secure!

On a shared public computer?
Log in with your UVa computing ID and a password you use for one of the compatible systems.

Applicant for admission or SCPS student? Use this option.
Network Infrastructure Components

- Configure Network Infrastructure for Certificates
  - 802.1x / EAP-TLS for Wireless Access
    - Radius Servers,
    - AuthZ (LDAP) integration

- VPN
  - Certificate-based authentication
  - LDAP integration for AuthZ

- Wired network opportunity
EAP-TLS Wireless Implementation

- Radius Servers
- LDAP Authorization
- Campus Network
  - User
  - Access Point
- User
VPN Implementation

- Campus Local Servers and Services
- Campus Network
- Internet
- Remote Computer
- Authorization (LDAP) Server
- VPN Concentrator
Network On-Boarding Automation

- Many schools have developed local tools
- UVa Tool, depending on platform, implements functions such as:
  - Certificate installation
  - Wireless configuration
  - Windows firewall
  - VPN settings
  - Security settings
  - Network registration
InCert™: Common Network On-Boarding Tool Development

- **Goals for InCert**
  - Automate on-boarding for workstations and mobile devices
    - Automatically configure network and wireless settings – campus and eduroam
    - Device registration, security configuration, etc.
  - Open community-sourced tool set
  - Life-cycle management of end user certificates
    - Built-in support for InCommon Certificate Service
  - Customizable without coding
    - Easy for campus to leverage just the pieces that meet local needs
  - Early support for at least Windows, MacOS, and iOS
  - Support for other campus needs (e.g., netreg, inventory)
InCert Tool Structure

Goals

- InCommon
- Comodo CA

Campus Server

- Campus AuthNZ
- Macintosh Client
- Windows Client
- iOS Interface
- Android Client
- Campus Logging, etc.
User Onboarding Process

Comodo CA

Campus Certificate Proxy

User Device

Guest Captive Portal (Software Download)

Guest/Bootstrap VLAN/SSID
Current Status

(Version 1.0 deliverables are a subset of the longer-term goals)

- **Version 1.0 Clients**
  - **Windows Client** – full initial scope
  - **iOS Web Service** – full initial scope
    - Wireless, Device PIN, Certificate, VPN
  - **Macintosh (OS-X) Web Service** – reduced scope
    - Wireless, AuthN Screen Saver, Certificate, VPN

- **Indiana University developing clients**
  - Much of the core functionality is already operational
<table>
<thead>
<tr>
<th>#</th>
<th>Description</th>
<th>Windows</th>
<th>Apple</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install a certificate and private key in PKCS12 format into the user’s native store. This includes the installation of intermediate certificates, handling user authentication, etc.</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
<tr>
<td>2</td>
<td>Download profile and configure wireless for EAP-TLS for Campus SSID.</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
<tr>
<td>3</td>
<td>Download profile and configure wireless for EAP-TLS for eduroam SSID.</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
<tr>
<td>4</td>
<td>Download and configure other campus wireless profiles.</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
<tr>
<td>5</td>
<td>Configure the workstation’s firewall.</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
<tr>
<td>6</td>
<td>Enforce a passcode or password policy; if the user deletes this policy requirement, delete the certificate; enforce an inactivity timeout. ²</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
<tr>
<td>7</td>
<td>Configure a password-protected screen saver.</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
<tr>
<td>8</td>
<td>Require password-based workstation login.</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
<tr>
<td>9</td>
<td>On each user login, check if certificate will expire in the next 30 days. If so, prompt the user to obtain a new certificate.</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
<tr>
<td>10</td>
<td>Computer MAC address registration (Wired and Wireless).</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
<tr>
<td>11</td>
<td>Ability for the user to rerun the tool as needed to fix settings (without obtaining a new certificate each time).</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
<tr>
<td>12</td>
<td>Customizable MSI installer.</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
<tr>
<td>13</td>
<td>XML-driven utility configuration with XSD schema.</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
<tr>
<td>14</td>
<td>Create a restore point.</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
<tr>
<td>15</td>
<td>Configure Windows Update.</td>
<td>✔ ⚫</td>
<td>✔</td>
</tr>
</tbody>
</table>

See [http://www.internet2.edu/incert/functionality.html](http://www.internet2.edu/incert/functionality.html) for details
Windows Tool

Verifying Security

- Setting system restore point
- Confirming administrator credentials
- Verifying system integrity
  Please wait while InCert scans your computer for viruses, trojans, or other types of malicious software.
- Checking Windows Security Center
- Checking anti-virus software
- Checking anti-spyware software

Configuring Computer

- Configuring network security
- Configuring screen saver
- Installing certificate
- Adding wireless profiles
- Registering computer
iOS and MacOS Tool

Select your site and enter your credentials to receive your iOS/OS X Configuration Profile.

Site:

**Indiana University**

Login-ID:

jaj

Password:

●●●●●●●

Last Name:

cred2

UVa Configuration...

University of Virginia

Verified

Install

Description

This profile configures iOS devices to connect to UVa network resources for University Faculty, Staff, and Students.

Signed

Internet2

Received

Apr 22, 2013

Contains

7 Certificates
Wi-Fi Network
VPN Settings
Password Policy

More Details
Getting Involved

- Testing and Deployment
  - 30 to 60 days
  - New Comodo CA update needed to support tools

- Contributing to the Windows/Apple tools
  - 60 to 90 days

- Android Developer
  - Now

- Contact: incert-info@internet2.edu
Background Information

- **Summary Document**
  - [https://www.incommon.org/cert/clientcerts.html](https://www.incommon.org/cert/clientcerts.html)
  - [http://www.internet2.edu/incert](http://www.internet2.edu/incert)
  - [https://spaces.internet2.edu/download/attachment/24577004/InCommonCertToolv2.pdf](https://spaces.internet2.edu/download/attachment/24577004/InCommonCertToolv2.pdf)
  - [https://spaces.internet2.edu/x/f66KAQ](https://spaces.internet2.edu/x/f66KAQ)

- **OS Requirements Table**
  - [https://spaces.internet2.edu/x/uQKnAQ](https://spaces.internet2.edu/x/uQKnAQ)

- **Client Certificate Roadmap**
  - [https://spaces.internet2.edu/x/7AN3AQ](https://spaces.internet2.edu/x/7AN3AQ)
• Questions / Discussion

• Thank you