

The InCert™ Project and Two-Factor Authentication

Multi-Factor Authentication Cohortium Meeting
November 27, 2013

Jim Jokl
University of Virginia

InCert: The Problem Space

- InCert addresses two independent but related issues
 - Stronger authentication can be hard to deploy
 - Passwords are painful to use, phishing is easy and commonplace
 - Enhanced authentication, to be used, must be as or more simple for users to use than normal passwords and add real security
 - Manual on-boarding of devices on to the campus network is hard
 - Device configuration for campus network (WLAN)
 - Device MAC address network registration
 - Security settings & device security testing
 - etc., etc.

Today's discussion focuses on InCert's MFA support capabilities

InCert and Assurance

- A Level of Assurance (LoA) generally requires
 - An *Identity Proofing* process that identifies the individual
 - A *Credential Issuance* process leveraging the identity proofing work to bind the credential to the end user
 - Credential technical properties
 - A sufficiently strong credential
 - Credential protection mechanisms (e.g., password memorization, token, etc.)
- InCert focuses on something we call “*Standard Assurance*”
 - Supports the use of stronger authentication technology for common campus applications

Digital Certificates



- Digital Certificates are a binding between a name and a cryptographic key pair
 - The binding is performed by a Certification Authority (CA) that is *trusted* by everyone
 - The CA digitally signs the certificate
- Some common certificate uses
 - Identifying web sites and supporting SSL encryption
 - Digital signatures for software distribution
 - Signed electronic mail
 - Authenticating users (and devices)
- Certificate-based authentication is immune from phishing attacks

Personal Digital Certificate Applications

- Common Uses for *Standard Assurance* Certificates
 - Web authentication, typically to campus Web SSO
 - 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>

Applications: Web SSO AuthN

On your computer?

Log in with your **UVa Digital Certificate**

[\(What's this?\)](#) | [Get one now!](#)

Log In

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.

UVa computing ID

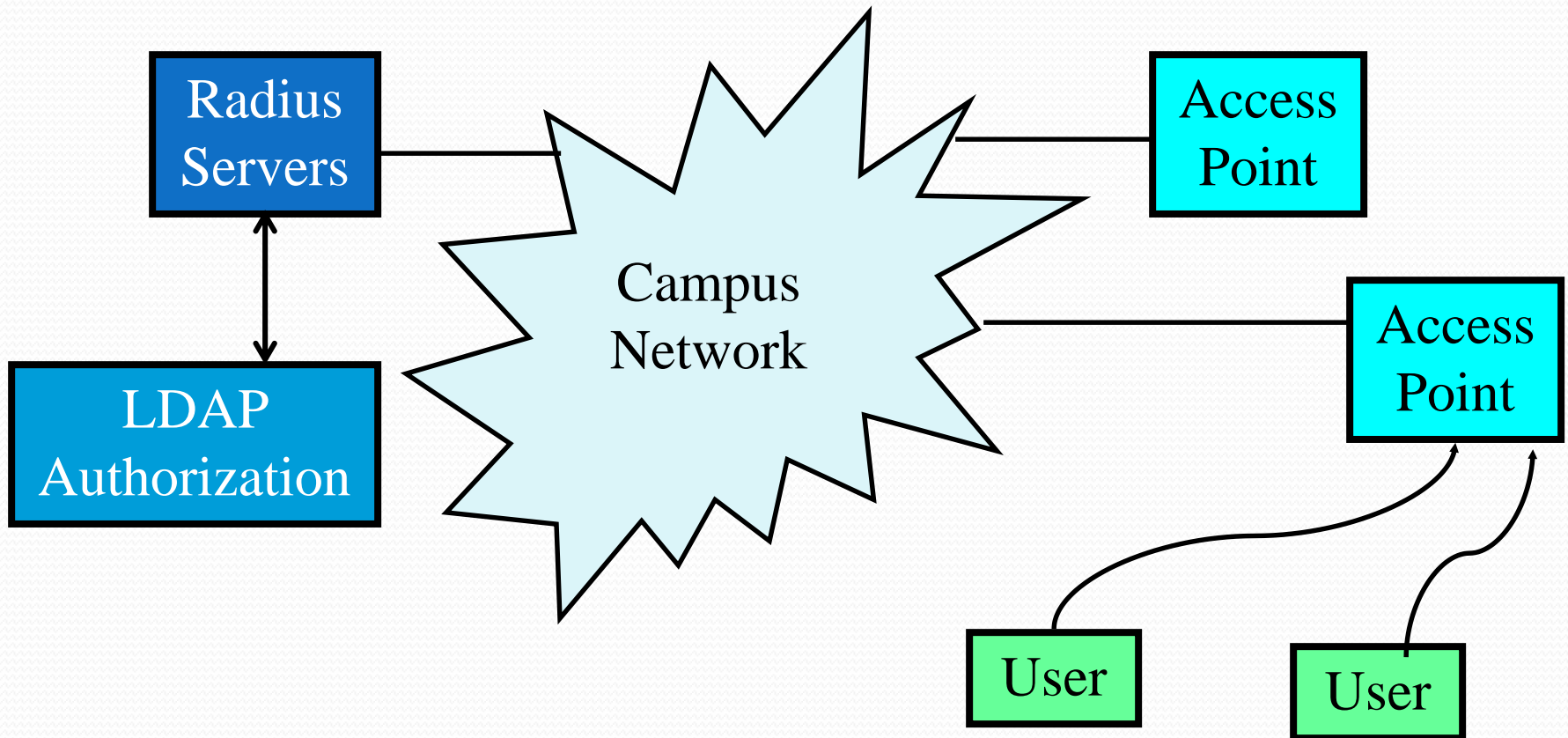
Password

Log In

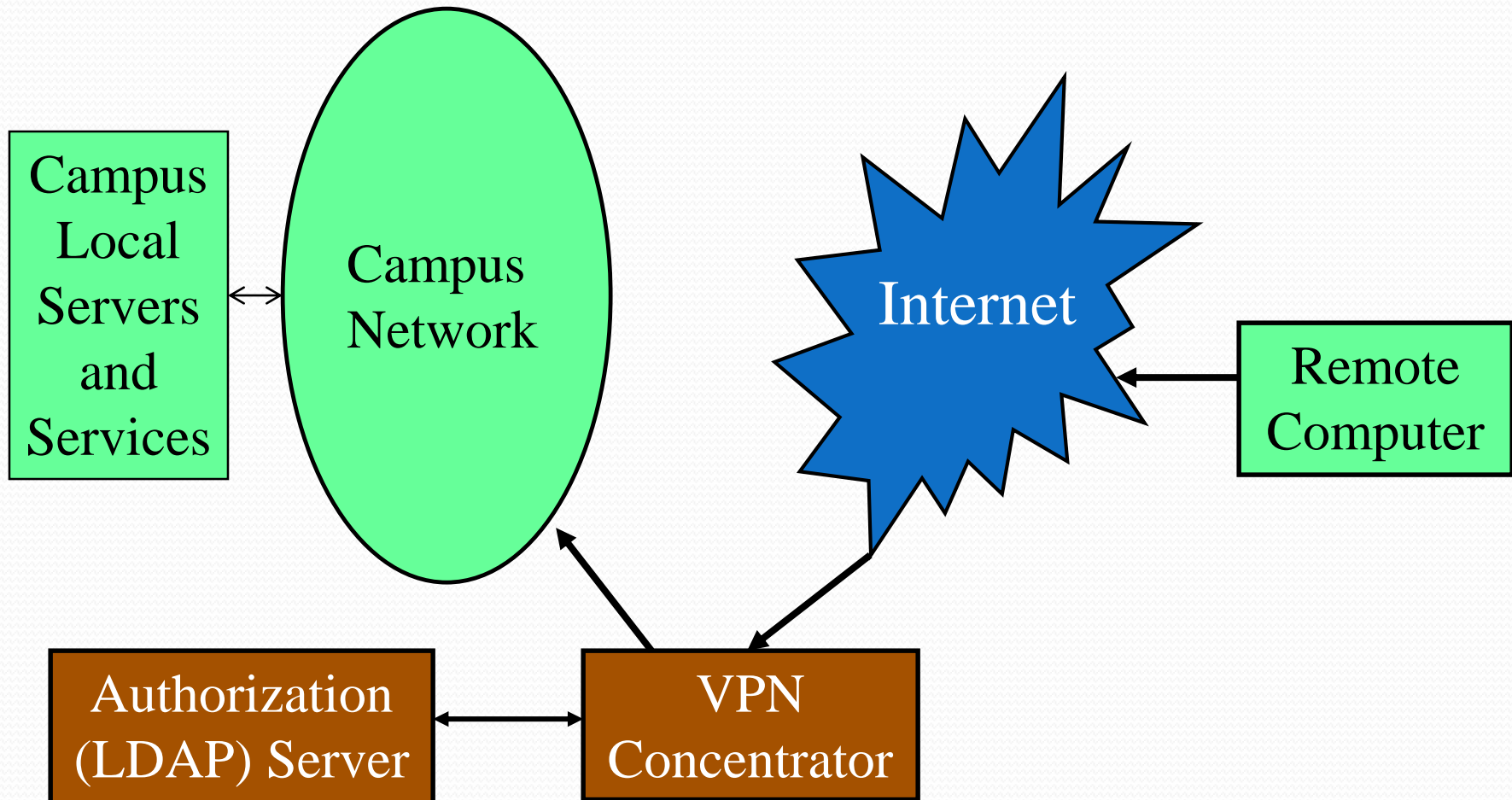
- At UVa

- We have used personal certificates for many years
 - Everyone has a certificate (or two)
 - Users need certificates for Wireless, VPN, etc.
 - Certificates are generally more convenient to use and much more secure than passwords
- Key to success: easy certificate lifecycle management
 - We use a Certificate Provisioning Tool

Applications: EAP-TLS Wireless AuthN



Applications: VPN AuthN



Usability and Enhanced Security

- **Web SSO Authentication**
 - No phishing
 - Easier to use (single click)
 - MFA – at least from an anti-phishing perspective, perhaps more
- **Wireless Authentication**
 - 802.1x / EAP-TLS for Wireless Access
 - No phishing
 - For end users, it just silently works
 - eduroam
- **VPN**
 - No phishing
 - Simpler for end users, single click with no password entry
 - MFA – at least from an anti-phishing perspective, perhaps more

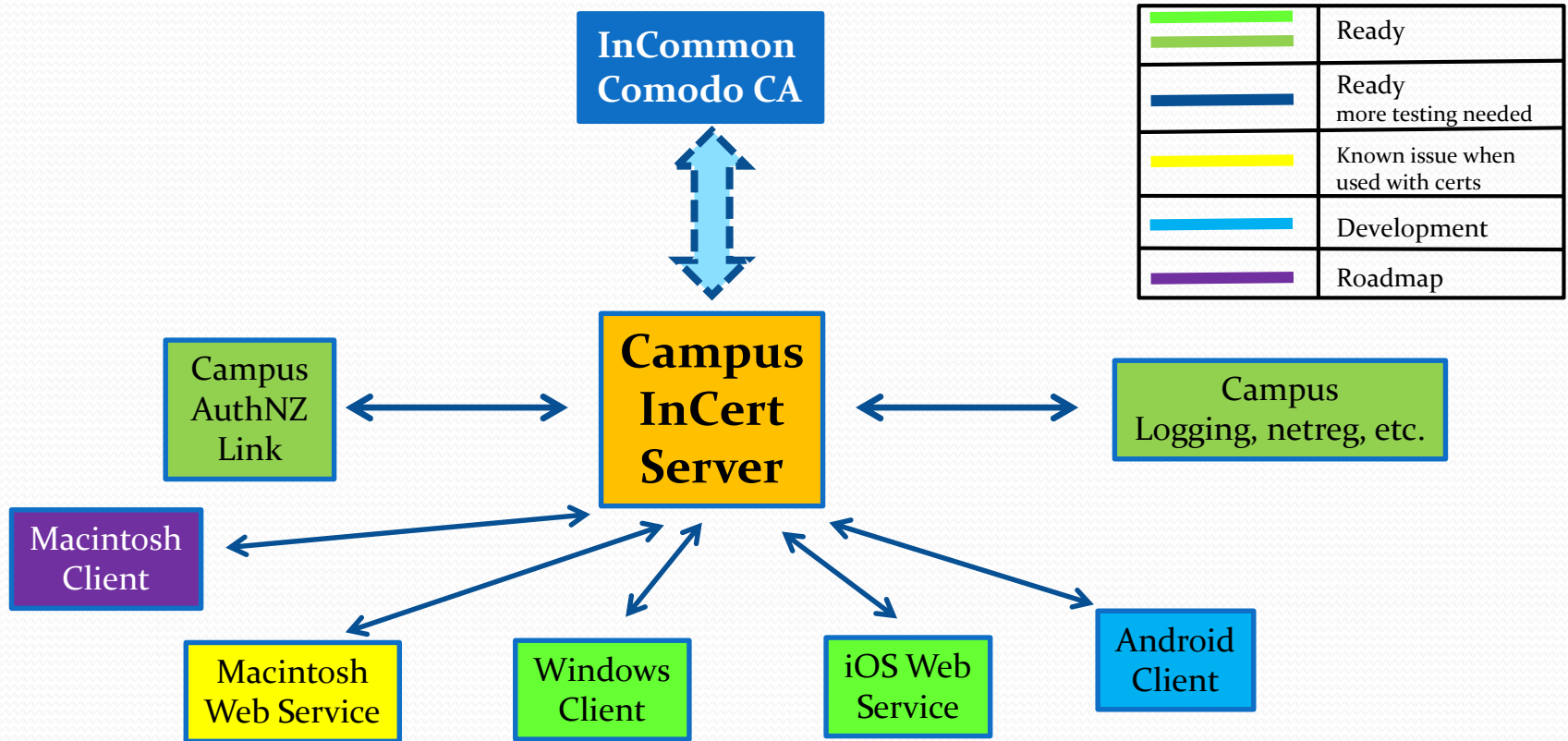
Challenges with Personal Certificates

- Why isn't everyone already using personal certificates?
 - Difficult to deploy to users
 - Certificate provisioning to end user devices
 - End user device configuration for certificate use
 - Certificate life-cycle management
 - Belief that certificates are difficult for users to use
 - Perception that certificates are for high assurance processes only
 - Lack of a business case
 - Passwords had been considered "good enough"

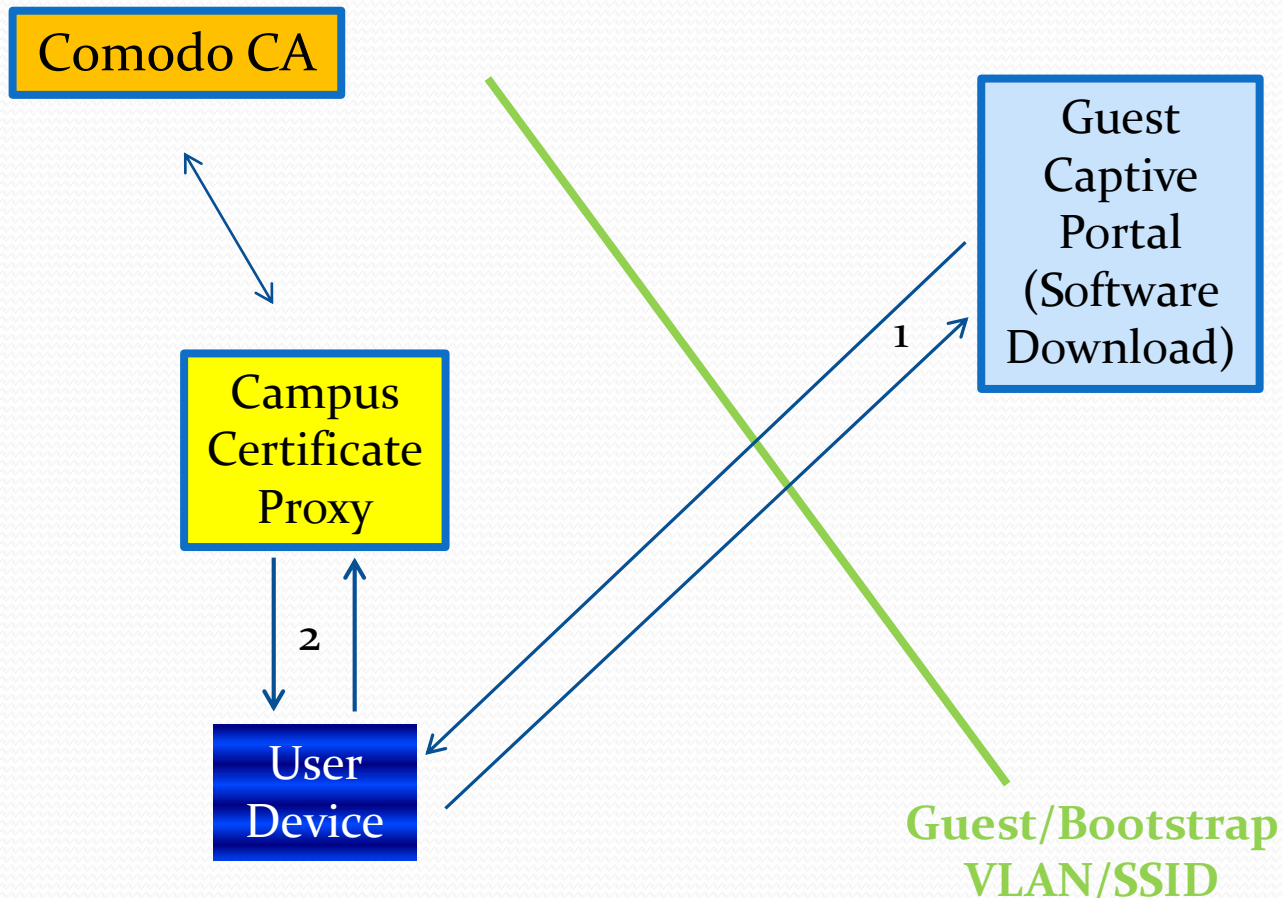
InCert: Common Device On-Boarding Tool Development

- Goals for InCert Project
 - Automate on-boarding for workstations and mobile devices
 - Automatically configure network and wireless settings
 - Campus SSIDs and/or 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 per-campus *without coding*
 - Easy for campus to leverage just the pieces that meet local needs
 - Early support for at Windows, MacOS, iOS, and now Android
 - Support for other campus needs (e.g., netreg, security, etc.)

InCert Tool Structure and Status



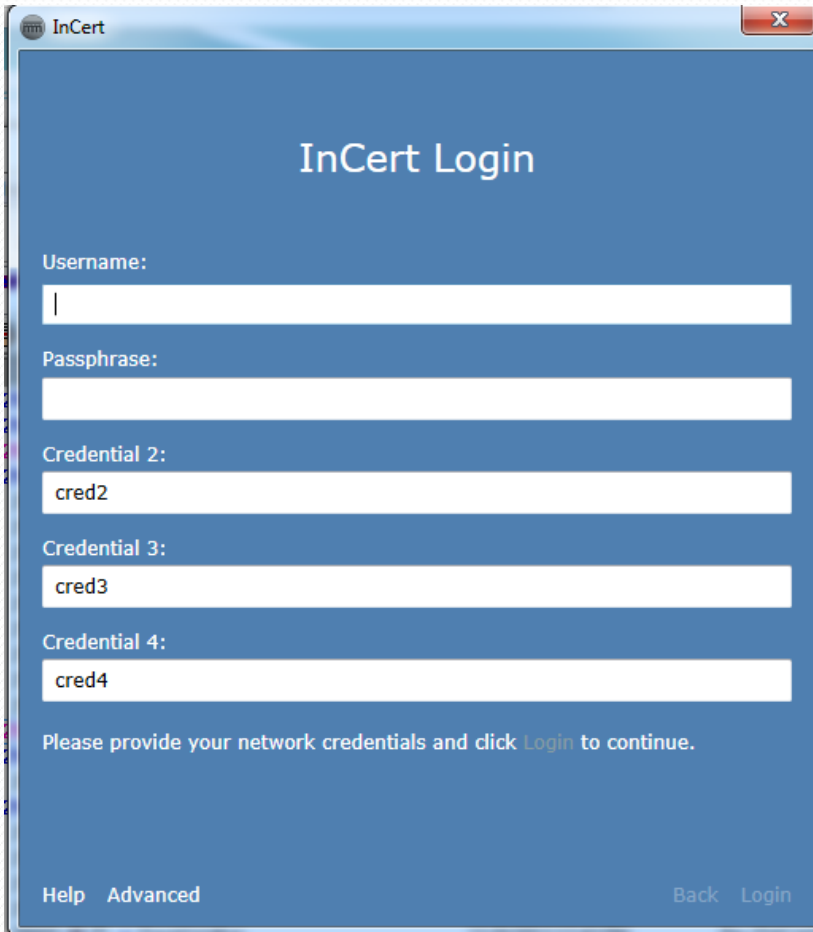
Typical Campus User/Device On-Boarding Process



#	Description	Windows			Apple	
		8 ¹	7	Vista	iOS	OS X
1	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.	✓	✓	✓	✓	✓
2	Download profile and configure wireless for EAP-TLS for Campus SSID.	✓	✓	✓	✓	✓
3	Download profile and configure wireless for EAP-TLS for eduroam SSID.	✓	✓	✓	✓	✓
4	Download and configure other campus wireless profiles.	✓	✓	✓	✓	✓
5	Configure the workstation's firewall.	✓	✓	✓		
6	Enforce a passcode or password policy; if the user deletes this policy requirement, delete the certificate; enforce an inactivity timeout. ²	✓	✓	✓	✓	✓ ³
7	Configure a password-protected screen saver.	✓	✓	✓		✓ ⁴
8	Require password-based workstation login.	✓	✓	✓		
9	On each user login, check if certificate will expire in the next 30 days. If so, prompt the user to obtain a new certificate.	✓	✓	✓		
10	Computer MAC address registration (Wired and Wireless).	✓	✓	✓		
11	Ability for the user to rerun the tool as needed to fix settings (without obtaining a new certificate each time).	✓	✓	✓		
12	Customizable MSI installer.	✓	✓	✓		
13	XML-driven utility configuration with XSD schema.	✓	✓	✓		
14	Create a restore point.	✓	✓	✓		
15	Configure Windows Update.	✓	✓	✓		

See <http://www.internet2.edu/incert/functionality.html> for details

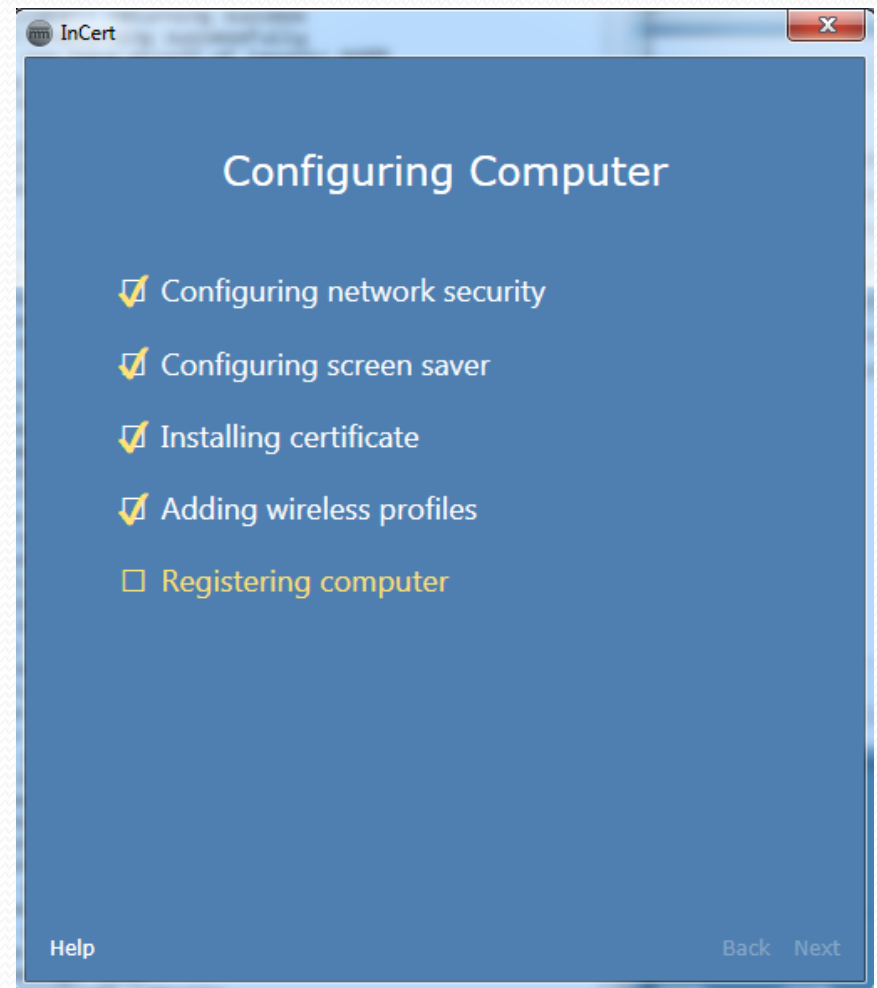
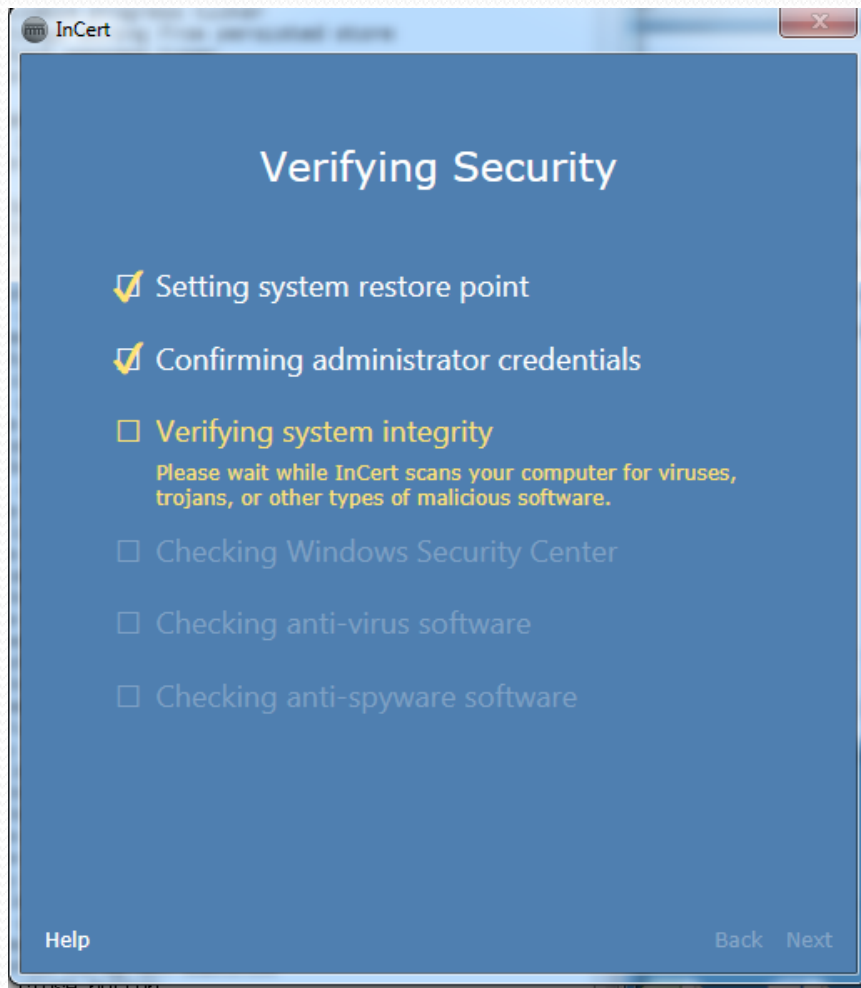
InCert Certificate Provisioning



The screenshot shows a web browser window titled "InCert" with a close button in the top right corner. The main content area has a dark blue background with the text "InCert Login" centered at the top. Below this, there are five input fields, each with a label to its left: "Username:" followed by an empty text box; "Passphrase:" followed by an empty text box; "Credential 2:" followed by a text box containing "cred2"; "Credential 3:" followed by a text box containing "cred3"; and "Credential 4:" followed by a text box containing "cred4". At the bottom of the form area, there is a line of text: "Please provide your network credentials and click [Login](#) to continue." In the bottom left corner, there are links for "Help" and "Advanced". In the bottom right corner, there are links for "Back" and "Login".

- Certificate Provisioning
 - Username and Password
 - Ability to add up to three additional shared secrets
 - ID Number
 - Security Questions
 - Date of Birth
 - etc.
- Enables credential issuing with more assurance than just a password

InCert Security



iOS and MacOS Tool

AT&T 3G 9:35 AM

InCert

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

AT&T 3G 10:22 AM

Cancel Install Profile

 **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

- Request for testers and feedback
 - We'll provide test accounts on incommontest.org
 - You will be issued certificates from the InCommon Comodo CA
- Client Testing
 - Windows client
 - iOS web service
 - Mac OSX Web Service
 - Note: Mac OSX certificate import bug and planned client
- Services / Demos
 - Device analysis
 - Web authentication
 - If you support eduroam on campus, testing certificate-based wireless authentication
- To become a tester, please email: incert-info@internet2.edu
 - We'll contact you after the Thanksgiving holidays
- Source code
 - The source code is slowly starting to become available
 - See: <https://github.com/Internet2/incert/>

InCert Background/Summary Information

- Summary Documents
 - <http://www.internet2.edu/vision-initiatives/initiatives/trusted-identity-education/incert/>
 - <https://spaces.internet2.edu/download/attachments/24577004/InCommonCertToolv2.pdf>
 - <http://internet2.edu/incert/functionality.html>
 - <https://spaces.internet2.edu/x/f66KAQ>
 - <https://www.incommon.org/cert/clientcerts.html>
- Demonstration Site
 - <https://certdevo.incommonest.org/>
- Screen movie of early version of Windows client
 - <https://spaces.internet2.edu/x/vAhOAg>
- Client Certificate Roadmap
 - <https://spaces.internet2.edu/x/7AN3AQ>

- Questions / Discussion
- Thank you