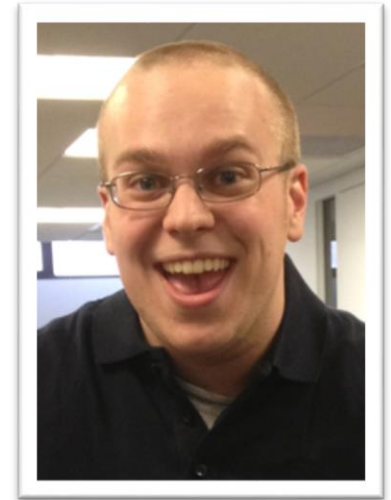


Real-world 802.1X Deployment Challenges

Tim Cappalli

3/13/14

- **Mobility Engineer, Brandeis University**
- **Wireless Infrastructure**
- **AAA / Role-based Access Control**
 - wired, wireless and remote networks



 @tcappy0707



- **6,000 students**
- **1,300 full time staff**
- **Smallest VHR university**
- **2,200 access points (mix 11n/11ac)**
- **5 mobility controllers**
- **320 edge switches, 92 stacks**
- **AAA: ClearPass Policy Manager**
- **eduroam**

What is EAP?

Common EAP Flavors

The Good and The Bad

Client Support

Challenges at Brandeis

Open Discussion – What challenges do you face?

802.1X

802.1X

IEEE STANDARD

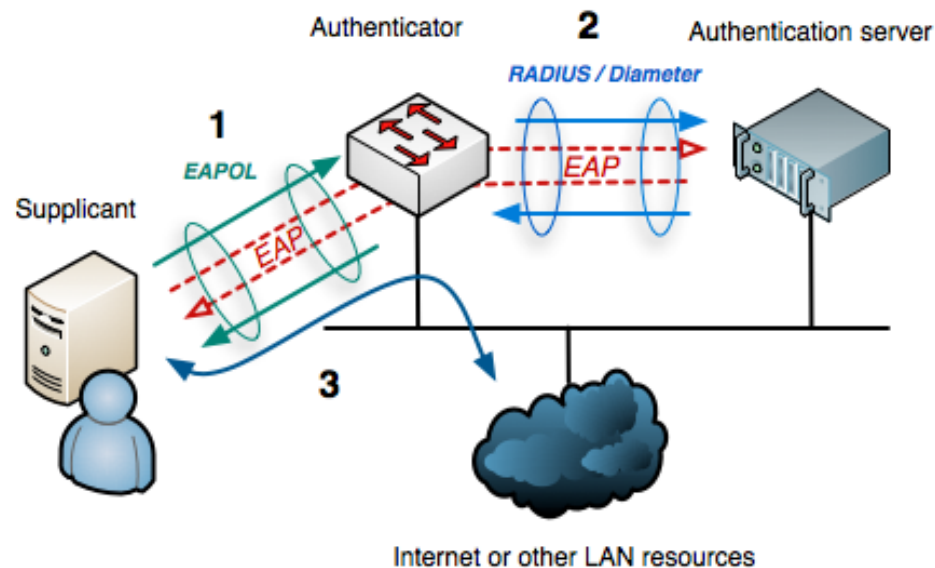
POLL

WHAT ARE YOU USING?

PEAP? TLS? TTLS?

- **Extensible Authentication Protocol**

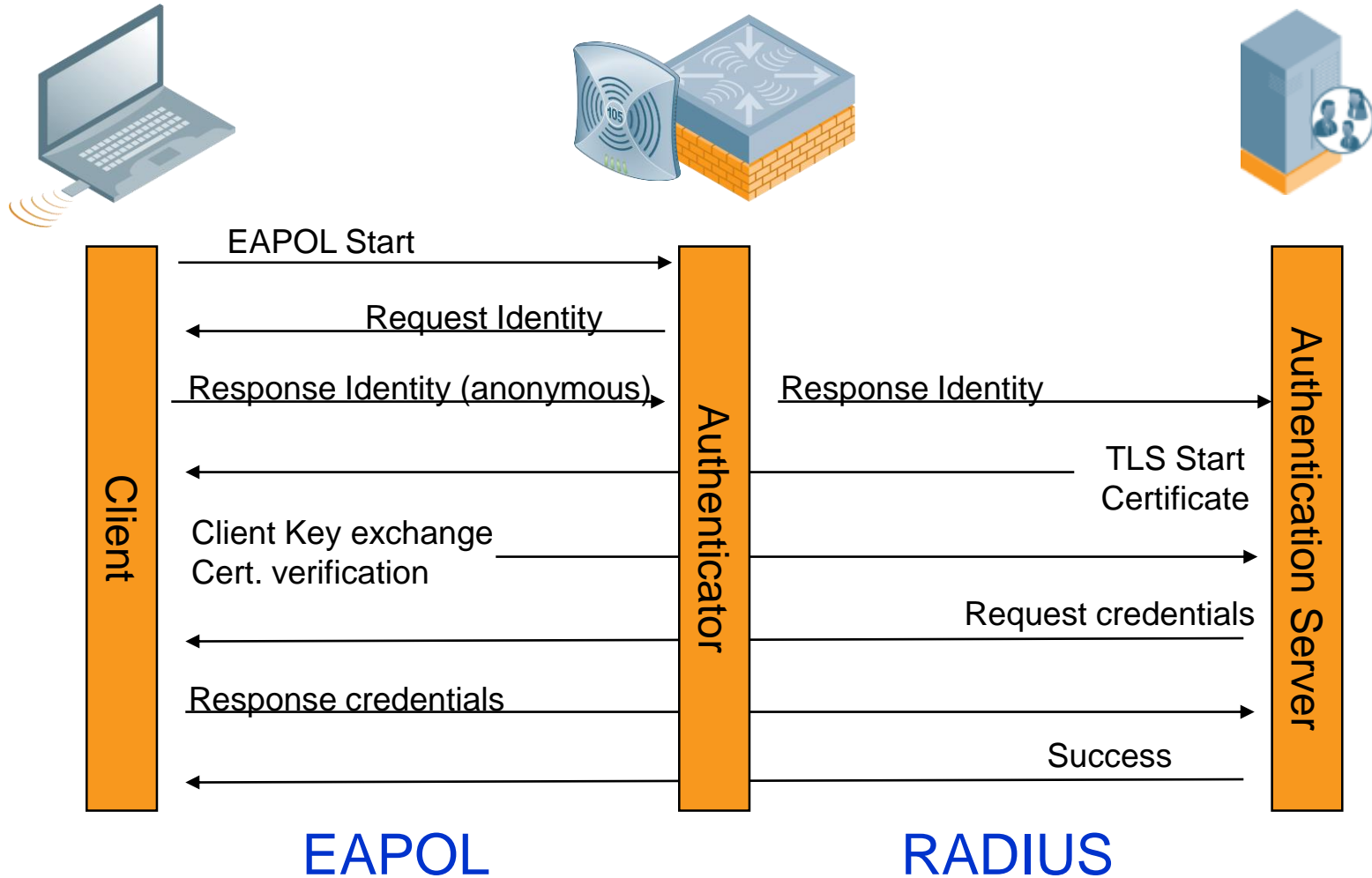
- 802.1X defines EAPOL
- Designed for Ethernet, adapted to 802.11



Arran Cudbard-Bell

EAP Transaction

ATMOSPHERE 2014



EAP FLAVORS

- **PEAP (Protected EAP)**
 - Uses a digital certificate on the network side
 - Password or certificate on the client side
 - Most common: PEAPv0/EAP-MSCHAPv2
- **EAP-TLS (EAP with Transport Layer Security)**
 - Uses a certificate on the network side
 - Uses a certificate on the client side
- **TTLS (Tunneled Transport Layer Security)**
 - Uses a certificate on the network side
 - Password, token, or certificate on the client side
 - Tunneled Diameter (CHAP, PAP), EAP

THE GOOD AND THE BAD

- **Device or User credential**
 - Revoke device access instead of user
- **Currently the strongest authentication method**
- **Most widely supported**
- **Extremely difficult to crack a 2048-bit RSA key**

- **Certificate distribution**
 - Enrollment or onboard process
 - Can be an administrative burden without proper tools
- **User familiarity**
 - Most users have no concept of a certificate
 - Username and password is the “standard”
- **Renewals**
 - Notifying users to renew before expiration
- **Changing certificate chain**
 - Not just “accept new certificate” for users

- **Username / password is familiar to users**
- **Users can “just get on” w/ valid credentials**
- **Second most widely supported**
- **Easy integration with AD (“free” NPS)**

- **Device credential on Windows AD-joined devices**
- **Passwords are weak!**
 - Users won't remember a truly secure password
- **Password expiration**
 - How do you handle AD password expiration for non-AD Windows machines?
- **Client must be configured correctly**
- **Not so easy with LDAP & Novell**
 - Limited PEAPv1/EAP-GTC native client support

- **EAP-GTC**
 - Cleartext, NT hash, MD5 hash, salted MD5 hash
 - SHA1 hash, Slated SHA1 hash, UNIX crypt
- **EAP-MSCHAPv2**
 - Cleartext, NT hash, LM hash

- **Make sure CA correspondence goes to more than one person!**
- **Nightmares for wireless only devices:**
 - Server certificate expiration
 - New chain
 - New server name
- **Push out new profiles/GPOs ahead of time!**



CLIENT SUPPORT



Native Client Support

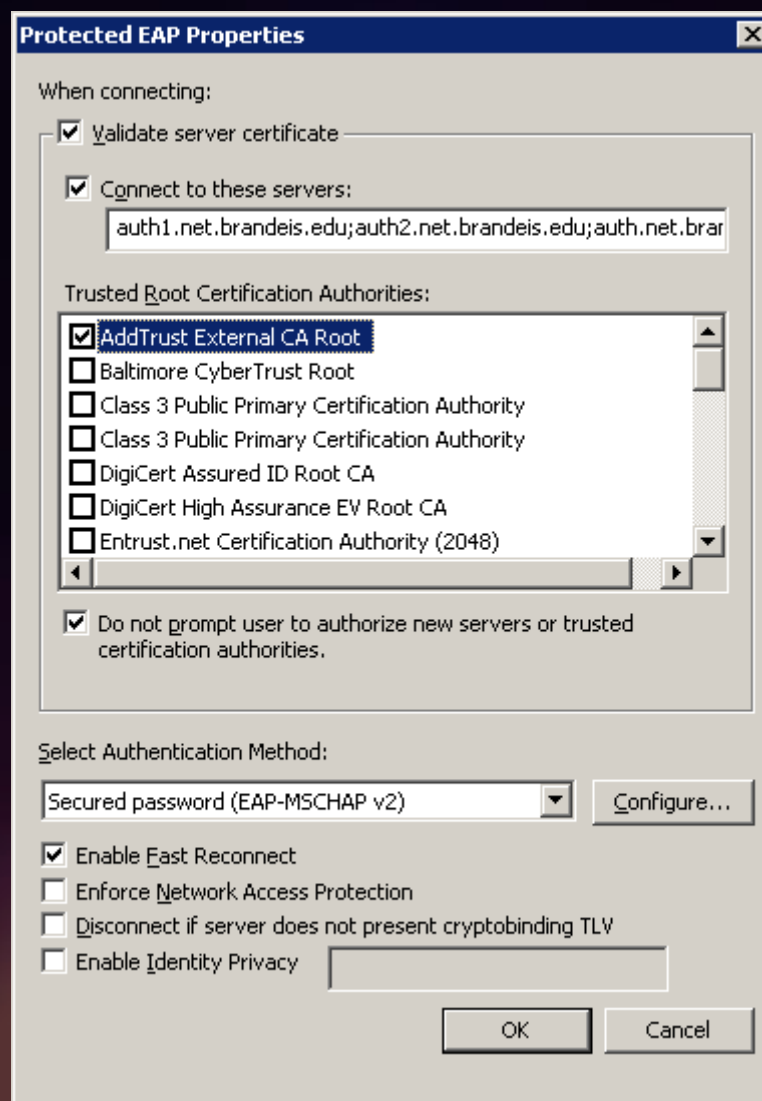
ATMOSPHERE 2014

	EAP-PEAP	EAP-TLS	EAP-TTLS
Windows 8	YES	YES	YES
Windows 7 / Vista / XP	YES	YES	NO
Mac OS X	YES	YES	YES
Linux	YES**	YES	YES
iOS	YES	YES	YES*
Android	YES**	YES	YES
Chrome OS	YES**	YES	YES**
Windows Phone 8.1	YES	YES (rumored)	UNK
Windows Phone 7/8	YES	NO**	NO
BlackBerry 10	YES	YES	YES
BlackBerry 7	YES	YES	YES

Native Client Support

ATMOSPHERE 2014

	EAP-PEAP	EAP-TLS	EAP-TTLS
XBOX 360	NO	NO	NO
XBOX One	MAYBE	MAYBE	MAYBE
PlayStation 3 & 4	NO	NO	NO
Nintendo Wii / Wii U	NO	NO	NO



Request Details

Summary

Input

Output

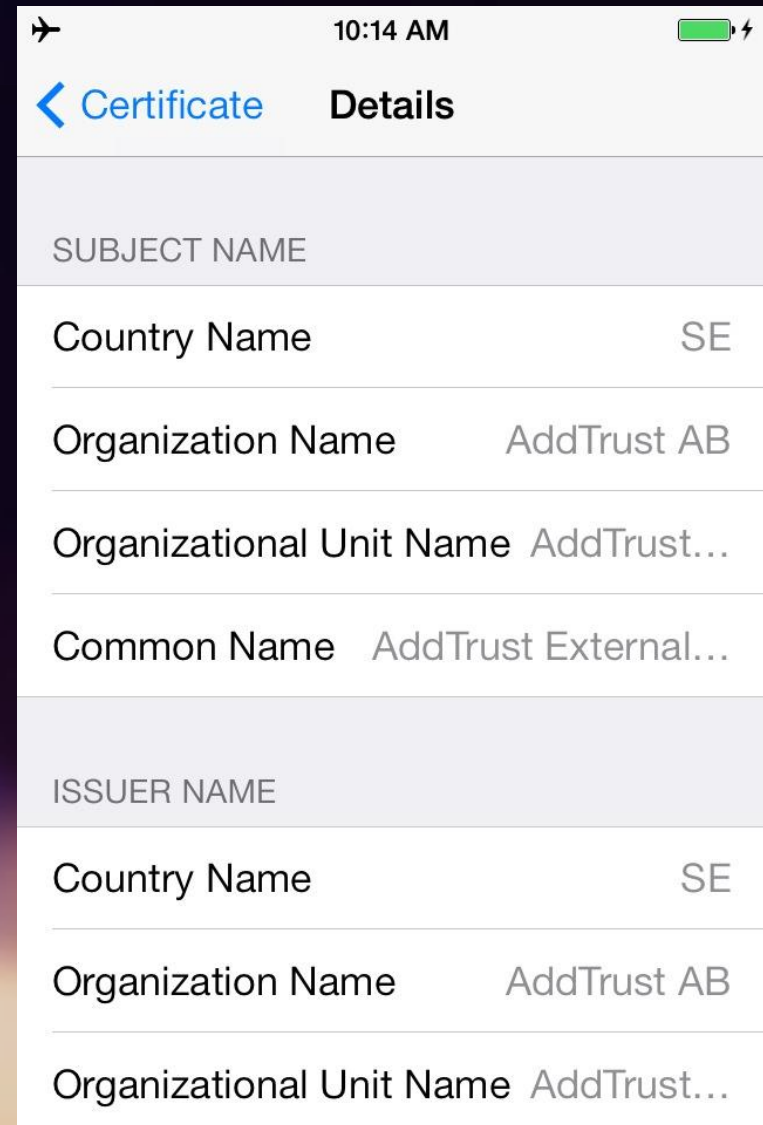
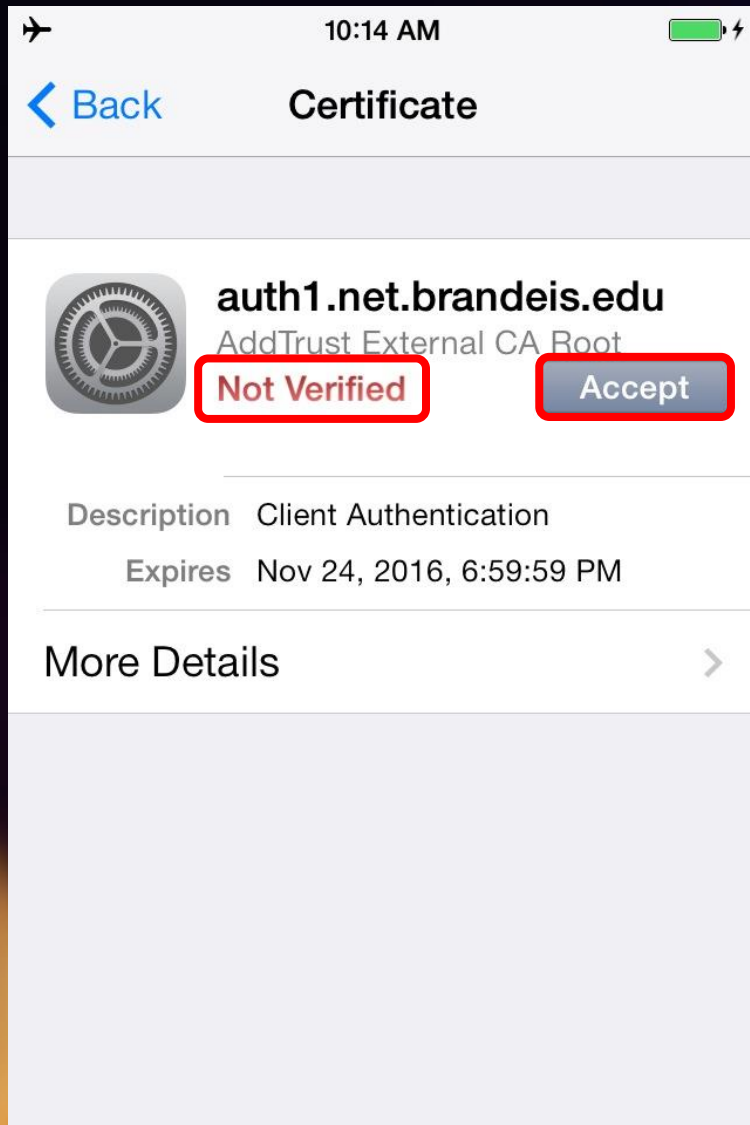
Alerts

Error Code:	215
Error Category:	Authentication failure
Error Message:	TLS session error

Alerts for this Request

RADIUS	EAP-PEAP: fatal alert by client - unknown_ca eap-tls: Error in establishing TLS session
--------	--

ATMOSPHERE 2014



Restrictions
Not configured

Global HTTP Proxy
Not configured

Web Content Filter
Not configured

Wi-Fi
1 Payload Configured

VPN
Not configured

AirPlay
Not configured

AirPrint
Not configured

Mail
Not configured

Exchange ActiveSync
Not configured

LDAP
Not configured

Calendar
Not configured

Contacts
Not configured

Subscribed Calendars
Not configured

Web Clips
Not configured

Service Set Identifier (SSID)
Identification of the wireless network to connect to

☐ **Hidden Network**
Enable if target network is not open or broadcasting

☒ **Auto Join**
Automatically join this wireless Network

Proxy Setup
Configures proxies to be used with this network

Security Type
Wireless network encryption to use when connecting

Enterprise Settings
Configuration of protocols, authentication, and trust

Trusted Certificates
Certificates trusted/expected for authentication

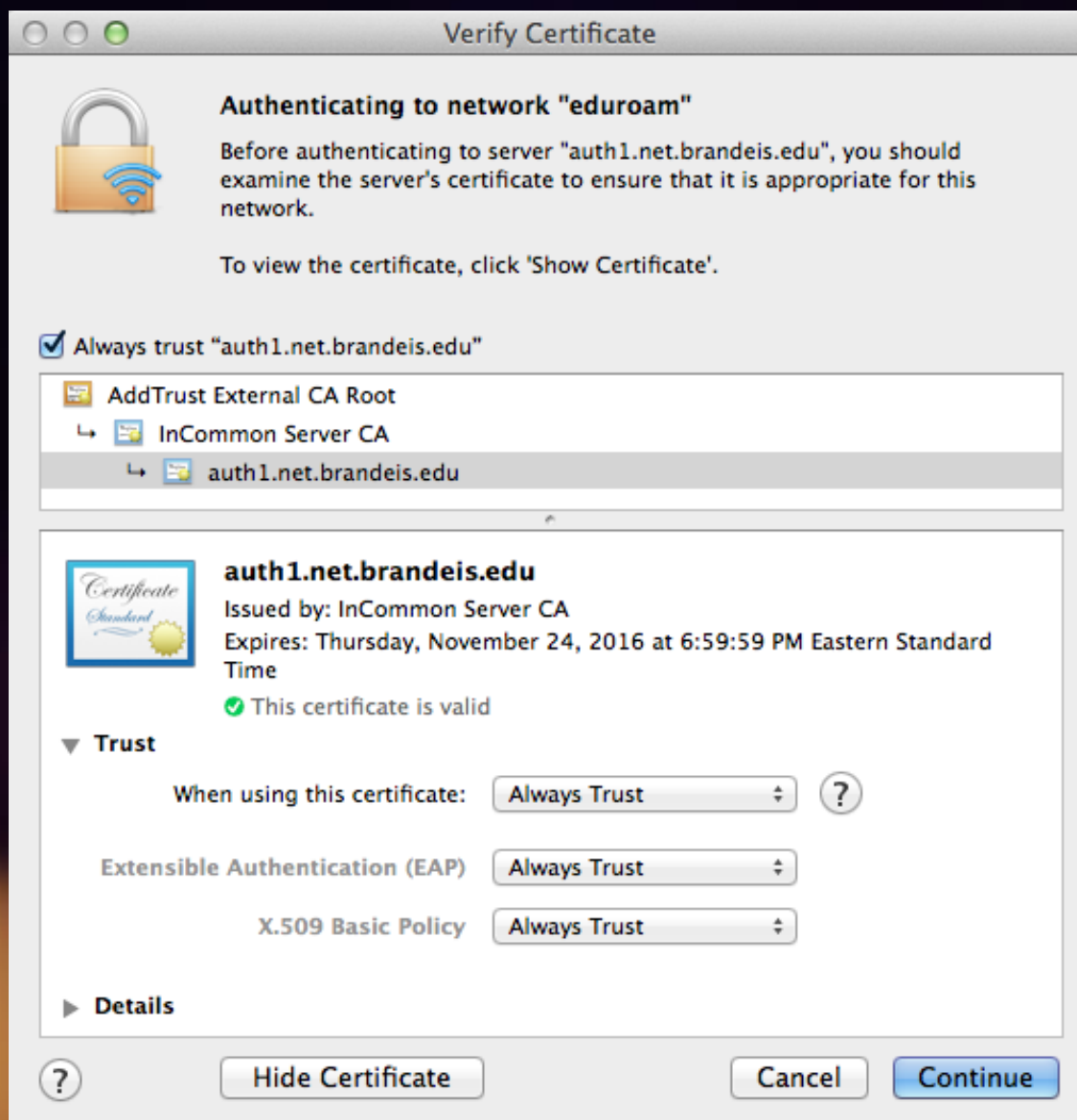
☒ InCommon Server CA
☒ AddTrust External CA Root

Trusted Server Certificate Names
Certificate names expected from authentication server


Network Type
Configures network to appear as legacy or Hotspot 2.0







← Networks

 eduroam

Continue connecting?

If you expect to find eduroam in this location, go ahead and connect. Otherwise, it may be a different network with the same name.

Hide certificate details

Server thumbprint: CE 62 7B EB 8C A8
BB F1 5F F7 AE F0 1C 9A E2 F6 80 69 88
60

Connect

Don't connect

Protected EAP Properties

When connecting:

☒ Verify the server's identity by validating the certificate

☒ Connect to these servers (examples: srv1;srv2;.*\,srv3\,com):

Trusted Root Certification Authorities:

- ☐ AddTrust External CA Root
- ☐ America Online Root Certification Authority 1
- ☐ Baltimore CyberTrust Root
- ☐ Class 3 Public Primary Certification Authority
- ☐ Class 3 Public Primary Certification Authority
- ☐ DigiCert Global Root CA
- ☐ DigiCert High Assurance EV Root CA

Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2) Configure...

☒ Enable Fast Reconnect

☐ Enforce Network Access Protection

☐ Disconnect if server does not present cryptobinding TLV

☐ Enable Identity Privacy

OK Cancel

Join Wi-Fi network

SSID:

eduroam

EAP method:

PEAP

Phase 2 authentication:

MSCHAPv2

Server CA certificate:

Default

Subject Match:

Default

User certificate:

Do not check

Identity:

Password:

Anonymous identity:

☒ Save identity and password

☐ Share this network with other users

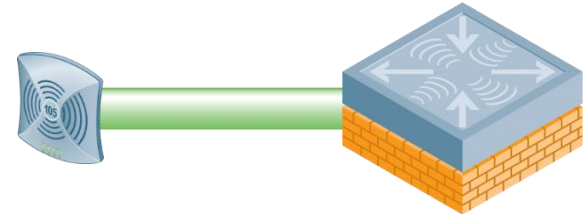
Connect

Cancel

VALIDATE SERVER CERT
Disabled



HospINET









radius1.hospital.org
Verisign



HospINET

wireless.hospital.org
Self-signed

 Configuration		 Windows	 MacOS X	 iOS	 Android	 Summary
Configure Wired: <input type="checkbox"/> Windows <input type="checkbox"/> MacOS X						
Wireless:						
SSID:	<input type="text" value="eduroam"/>					
Security Type:	<input type="text" value="WPA2 with AES"/>					
Network Type:	<input type="text" value="Enterprise"/>					
Hidden Network:	<input type="checkbox"/>					
SSIDs To Delete:	<input type="text" value="brandeis-open"/> <input type="text" value="lts-test"/> <input type="text" value="brandeis_voice"/> <input type="text" value="brandeis_guest"/>					Add SSID <input type="button" value="Remove"/>
Authentication Profile:						
Outer Identity:	<input type="text"/>					
Trust:						
Validate Server's Certificate:	<input checked="" type="checkbox"/>					
Servers To Trust:	<input type="text" value="auth.net.brandeis.edu"/> <input type="text" value="auth1.net.brandeis.edu"/> <input type="text" value="auth2.net.brandeis.edu"/> <input type="text" value="auth-dev1.net.brandeis.edu"/>					Add Radius Server <input type="button" value="Remove"/>
Allow User to Accept Other Servers:	<input type="checkbox"/>					
Trusted Root Certificate:	<input type="text" value="AddTrust External CA Root"/>					Add Certificate
Use Additional Trusted Certificates:	<input type="checkbox"/>					

Define Networks
Deploy
Advanced
Manage Account
Support

Network: 7

Summary
Windows XP
Windows Vista & Greater
Mac Tiger
Mac 10.5 & Greater, iOS
Ubuntu
Android
C

Windows Vista & Greater

The profiles below specify the configuration settings necessary for a user's machine to gain network access when using Win

+
Vista Support:
Enabled

+
Windows 7 Support:
Enabled

+
Windows 8 Support:
Enabled

+
Windows 8.1 Support:
Enabled

Wireless Connections

Behavior

- The user will be prompted for credentials beforehand.
- No custom scripts are defined.

Application Settings

- Wireless utilities need to be disabled.
- Root CA 'Go Daddy Class 2 Certification Authority' needs to be installed.
- Root CA 'Go Daddy Root Certificate Authority - G2' needs to be installed.
- Root CA 'Go Daddy Secure Certification Authority' needs to be installed.
- The Security Center service needs to be started. (Optional)
- 'Windows Auto Update' needs to be enabled. (Optional)
- 'Firewall' needs to be enabled. (Optional)
- Antivirus needs to be running and up-to-date. (Optional)
- Your computer's clock appears to be incorrect. (Optional)
- Anti-Spyware needs to be running. (Optional)
- 'WLAN AutoConfig Service' needs to be enabled.

+ Add application settings

Network Settings

- SSID '...' needs to be configured.
- 'Wireless Phy Type' needs to be set to 'Any'. (Optional)
- 'IPv6 Protocol state' needs to be disabled.
- 'Auto Switch' needs to be disabled.
- 'Show Icon In Notification Area' needs to be enabled.

+ Add network settings

Authentication Settings

- 'Authentication Mode' needs to be set to 'User Only'.
- 'Supplicant Mode' needs to be set to 'Compliant'.
- EAP Type 'PEAP' needs to be selected.
- 'Validate Server Certificate' needs to be enabled.
- 'Fast Reconnect' needs to be enabled.
- 'Disconnect if no cryptobinding' needs to be disabled.
- 'Authentication Method' needs to be set to 'Secured password (EAP-MSCHAPV2)'.
- Connect to server needs to be set to
- 'Do not prompt to authorize new server' needs to be enabled. (Optional)
- 'Automatically use Windows logon' needs to be disabled.
- Trusted Root CA '...' Certification Authority' and '...' Root Certificate Authority - G2' and '...' Secure Certification Authority' needs to be selected.
- 'Cache User Information' needs to be enabled.

COURTESY: LEE BADMAN, SYRACUSE UNIVERSITY

WHAT'S BRANDEIS DOING?

- **Training support staff**
 - Explaining the different networks
 - Giving access to troubleshooting tools
- **Empowering* users**
 - Making it interactive
 - Making it user friendly
- **Planning for some type of onboarding**
- **Exploring EAP-TLS**
 - Using network and systems group as PoC for access to secure management networks

Error Code:	215
Error Category:	Authentication failure
Error Message:	TLS session error
Alerts for this Request	
RADIUS	EAP-PEAP: fatal alert by client - unknown_ca eap-tls: Error in establishing TLS session

*attempting

Brandeis University

*get connected!*

Follow these steps to connect to **eduroam**, the Brandeis secure network for your laptop, tablet, and phone.

1. Download [brandeis-eduroam.mobileconfig](#).
2. Click **Continue** to install the wireless profile.
3. Enter **username@brandeis.edu** for your username, enter your Brandeis password, and click **Install**.
4. Select **eduroam** from your list of available networks.



[Library & Technology Services](#) ○ [About eduroam](#) ○ [Help](#)

What's Brandeis Doing?

ATMOSPHERE 2014



brandeis_open	59.1%
brandeis_secure	33.9%
brandeis_guest	3.8%
eduroam	3.1%

3/15/13



eduroam	34.9%
brandeis_open	32.9%
brandeis_secure	28.2%
brandeis_guest	4.1%

10/3/13

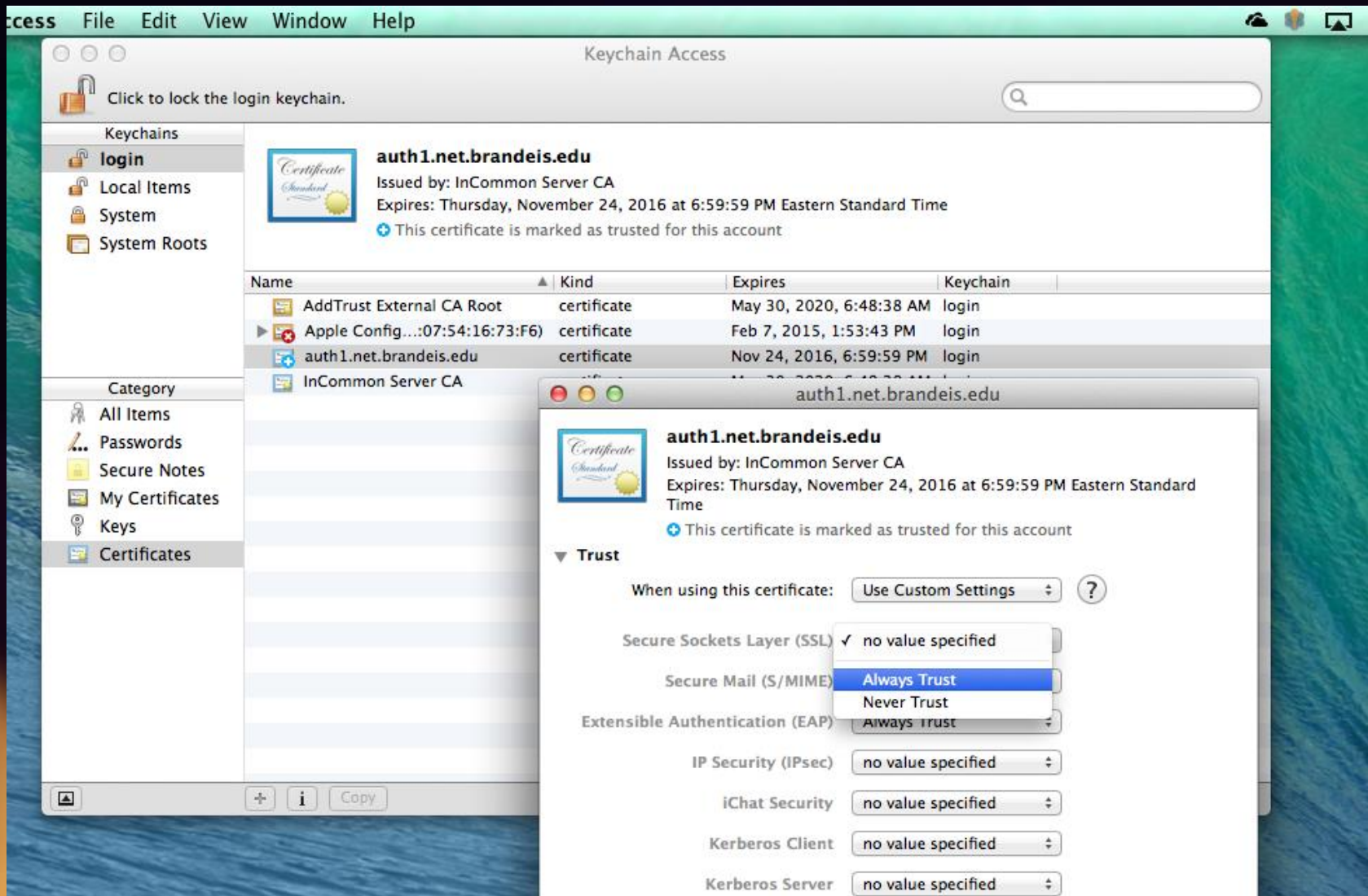


eduroam	69.1%
brandeis_secure	23.1%
brandeis_open	5.7%
brandeis_guest	2.1%

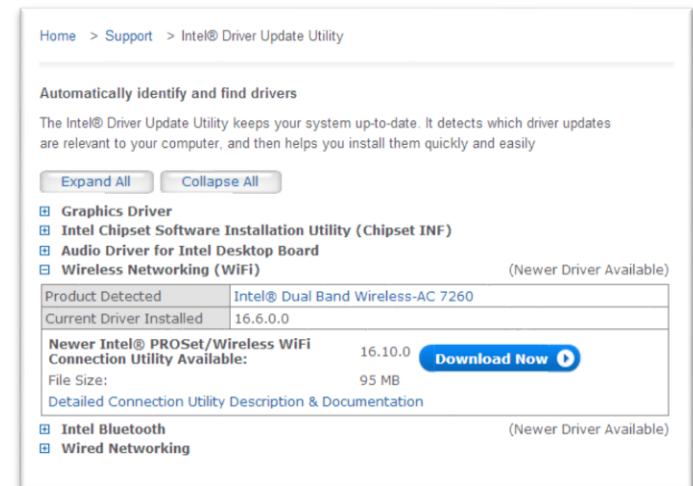
3/5/14

Know the audience

ATMOSPHERE 2014

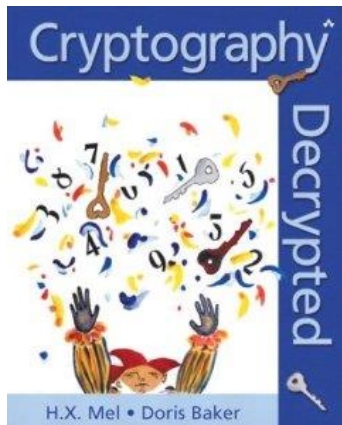


- **Ensure support staff understand the value of client configuration tools**
- **Utilize a configuration utility**
 - Teaching help desk, “When in doubt, run QuickConnect”
- **Utilize driver detection tools**
 - Intel Driver Update Utility



OPEN DISCUSSION

- **Simply put: How does certificate-based authentication work?** (Network World, 3/10/14, Aaron Woland)
- **Cryptography Decrypted** (Amazon)



ATMOSPHERE 2014

THE COSMOPOLITAN OF LAS VEGAS

MARCH 10-14, 2014

Thank You
