eduroam/TLS
some thoughts on EAP-TLS in eduroam®

Milan Sova
CESNET

Fall Internet2 Meeting 2011
Raleigh, NC
eduroam® Architecture

Top Level

.nl

realm1.nl

.cz

realm2.cz

.lu

realm3.lu

user@realm2.cz
eduroam® Architecture

Top Level

.nl

realm1.nl

.cz

realm2.cz

.lu

realm3.lu

user@realm2.cz
eduroam® RADIUS configuration

- IdP level
  - local realm(s): process
  - others: forward up

- higher level
  - realm of subordinate RADIUS: forward down
  - others: forward up

- top-level:
  - known realm: forward down
  - other: error
Issues

- routing loops
- real world does not follow DNS hierarchy
  - .edu, .org, .net within national eduroam members
  - exceptions at top-level national-level RADIUSes
- dependency on connection quality of several independent hops (UDP!)
  - authentication timeouts (UDP!)

=> eduroam/TLS (one of the approaches)
eduroam® Architecture

Top Level

.nl
 realm1.nl

.cz
 realm2.cz

.lu
 realm3.lu

user@realm2.cz
eduroam/TLS Architecture

Top Level

.nl
realm1.nl

.cz
realm2.cz

.lu
realm3.lu

Revocation

TLS/user@realm2.cz

CA 1

PKI
eduroam/TLS History

- ideas from 2007
- issues to solve
  - co-existence with legacy eduroam®
    - TLS users names prefixed with “TLS/”
      - “TLS/user123@cesnet.cz” vs. “user456@surfnet.nl”
  - client certificates deployment
    - “federated CA” prototype
  - RADIUS server revocation checking
    - off-the-shelf OpenSSL calls require server restart to reload CRL
    - showstopper at the time
Issues Revisited

- client certs deployment
  - federated CAs commonly used (TCS, CILogon,...)
- revocation checks
  - FreeRADIUS 2.1.11 (June 2011) supports OCSP
Client configuration deployment

- eduroam CAT
  - eduroam configuration assistant tool
  - GÉANT3 JRA3 T1
- portal providing eduroam® configuration based on user input:
  - home organization
  - device OS/supplicant sw
- possible integration with certificate issuing portal might improve user experience
This is a service under preparation, do not expect it to work.

Welcome to CAT
the eduroam Configuration Assistant Tool

View this page in Deutsch English(GB) Español Hrvatski Polski

Selected institution: moretesting select another

Choose an installer to download

- MS Windows 7
- MS Windows Vista
- MS Windows XP SP3
- Apple Mac OS X Lion
- Apple iOS mobile devices
- Welcome Letter
- Test
Conclusions

• *eduroam/TLS* technically feasible today
• even easier with the centralized EAP-TLS server
  but don't forget:
• interoperability with legacy *eduroam®*
• blacklisting at the SP side