Centralized Client Certificate Issuing System
- extension for DEAS -

Hideaki Goto  NII / Tohoku University
Tomo Niizuma  Tohoku University
Outline

- Centralized eduroam IdP service (Delegate Authentication System, DEAS)
  - Simplifies the eduroam system in the country
    - For better stability
    - Reduces RADIUS IdP deployment costs

- Client Certificate Issuing System
  - Simple and secure AuthN by EAP-TLS
  - Supports certificate downloads by end-users
  - Supports the disruption- / disaster-tolerant eduroam architecture (TF-MNM in Malaga, Oct. 2013)

- Online Sign-up System
  - End-user sign-up with email-based user validation
Easy-to-join eduroam system

Delegate Authentication System (DEAS) or Shibboleth-based eduroam account issuer

Institution’s RADIUS server

national RADIUS

national IdP service

<secret key 1>

auth requests

RADIUS proxy

<secret key 2>

RADIUS IdP

access points

AP system by inst. or ISP/carrier
Centralized / cloud IdP service

- Deploy IdP services at some ISPs for their customer institutions, geographically distributing the AuthN system for higher availability and efficiency.
Delegate Authentication System since 2008

DEAS (centralized / clustered)

RADIUS server

Institutions

DEAS (centralized / clustered)

FreeRADIUS
PostgreSQL
Perl CGI prog.

Manual account issue requests by inst. administrators.
- The system can be used even without IdM or fed.
- Issuing Guest IDs is possible.
- Manual ID distribution could be a burden.

eduroam

24 inst. / 60 members = 40.0% as of Feb. 2014

manual ID distribution
Client Certificate Issuing System

- Simple and secure AuthN by EAP-TLS
- Supports certificate download by end-users
- Supports the disruption-/disaster-tolerant eduroam architecture (TF-MNM in Malaga, Oct. 2013)

Steps:

- An inst. admin downloads a user account list, and passes the eduroam ID/PW pairs to the users.
- A user logs on to the web interface using the ID/PW.
- The user types in a passphrase for cert. installation.
- The user downloads the issued client certificate, and installs it on the terminal.
- Upon any incident, the inst. admin can lock the ID/PW and add the cert. to CRL.
• **email-addr.-based user validation.** (anti-spam, anti-bot)
• Request routing based on the email address with the institution’s domain name.
• Manual approval / rejection by the inst. admin., and ID/PW download by the user.
ID federation in the central IdP service

Central IdP service

RADIUS server

Client cert.

(PKCS#12)

GakuNin

ID/PW

eduroam

ID/PW

email account

Online sign-up by user & manual approval by inst. admin

ID/PW issue req. by inst. admin

cert. issue req. by user

Login via Shibboleth & cert. issue req.

Login via Shibboleth & ID/PW issue req.