

# Hosting 1,200+ organizations in eduroam

Hideaki {Goto, Sone}  
NII / Tohoku University, Japan





## A great challenge ...

How many higher education institutions are there in Japan?

1,200+ (govt. survey in year 2008)

- 765 universities (86 national, 90 public)
- 481 two-year colleges and vocational colleges

eduroam deployment:  $11 / 1200 = 0.9\%$



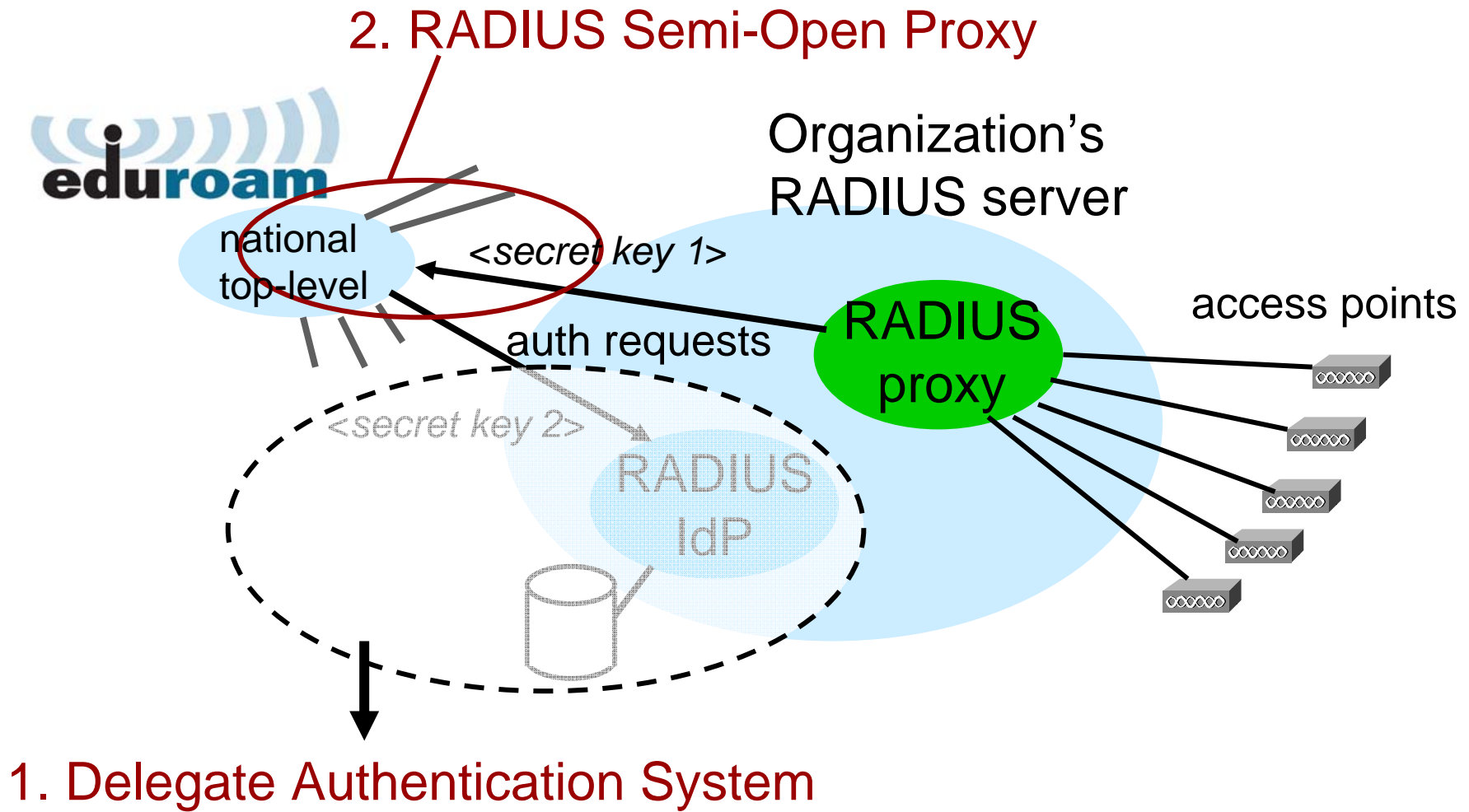
- Problems

- A large number of universities (1,200+)
- Difficulties in RADIUS deployment

- Solutions

- Federated Delegate Authentication System  
with centralized RADIUS server
  - remove RADIUS IdP at each organization
  - Federation using Shibboleth
  - simplify RADIUS tree (higher stability)
  - solve some privacy and security issues
- RADIUS Semi-Open Proxy
  - make eduroam AP deployment easy
  - reduce the work at the eduroam JP office

# A modified eduroam system





## Problem details in large-scale deployment

- Difficult and laborious configurations of RADIUS / APs at each organization.
- Difficulties in newly constructing an “eduroam account database” or making a RADIUS-IdM bridge for each organization.
- Many universities do not have Federated IdM yet.
- Laborious work for organization connection.
  - A lot of paper work
  - RADIUS configuration support
  - Connection testing
  - Troubleshooting ... etc.

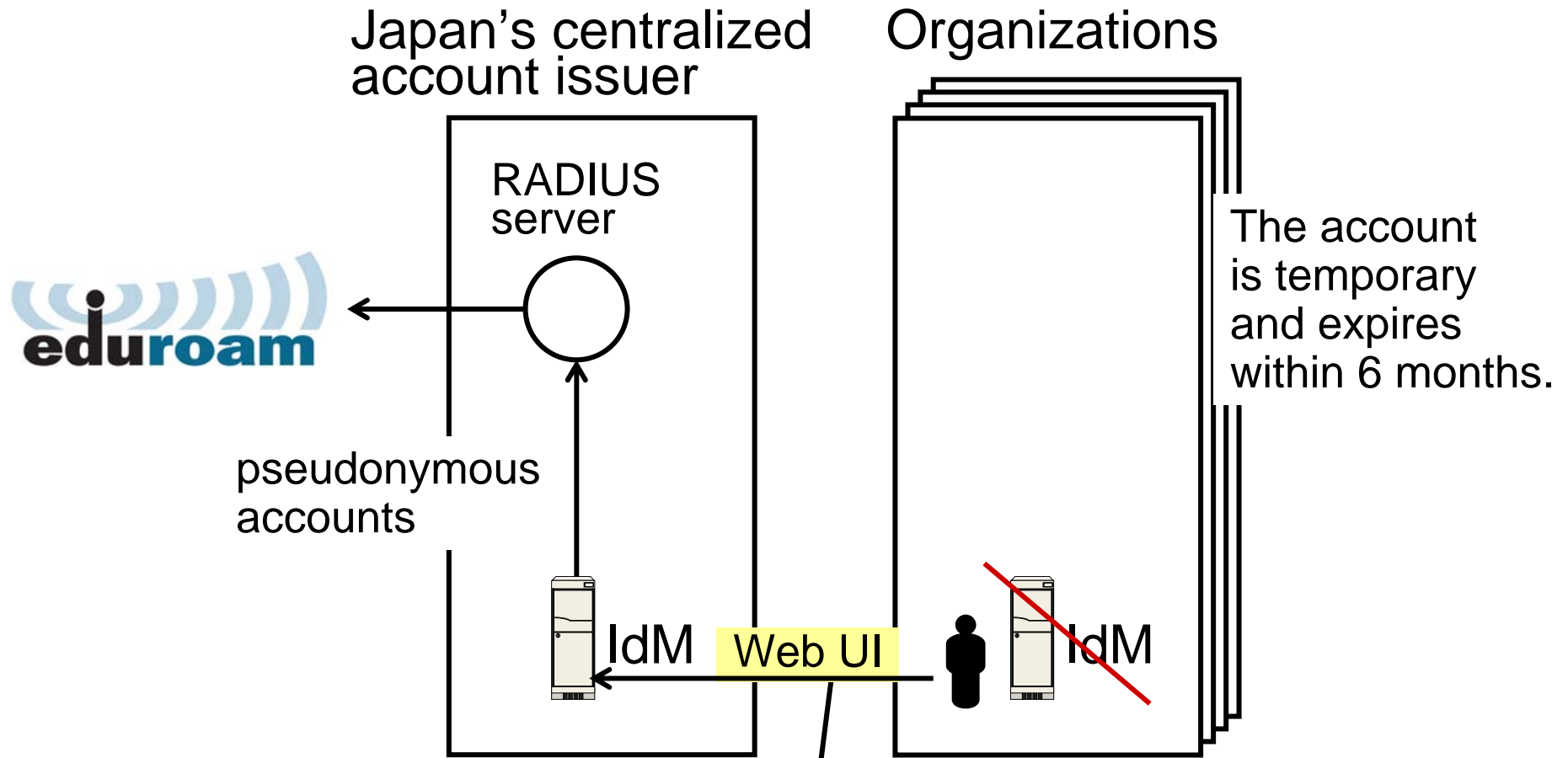
*Impossible to deal with hundreds of organizations!* 5



# Federated Delegate Authentication System

- Delegate Authentication System
  - Account Issuer as an SP of the UPKI inter-university federation
  - Centralized RADIUS server to simplify the RADIUS proxy tree
  - 3 types depending on the needs and federation level
- Pseudo-anonymized, fixed-term, and traceable roaming IDs

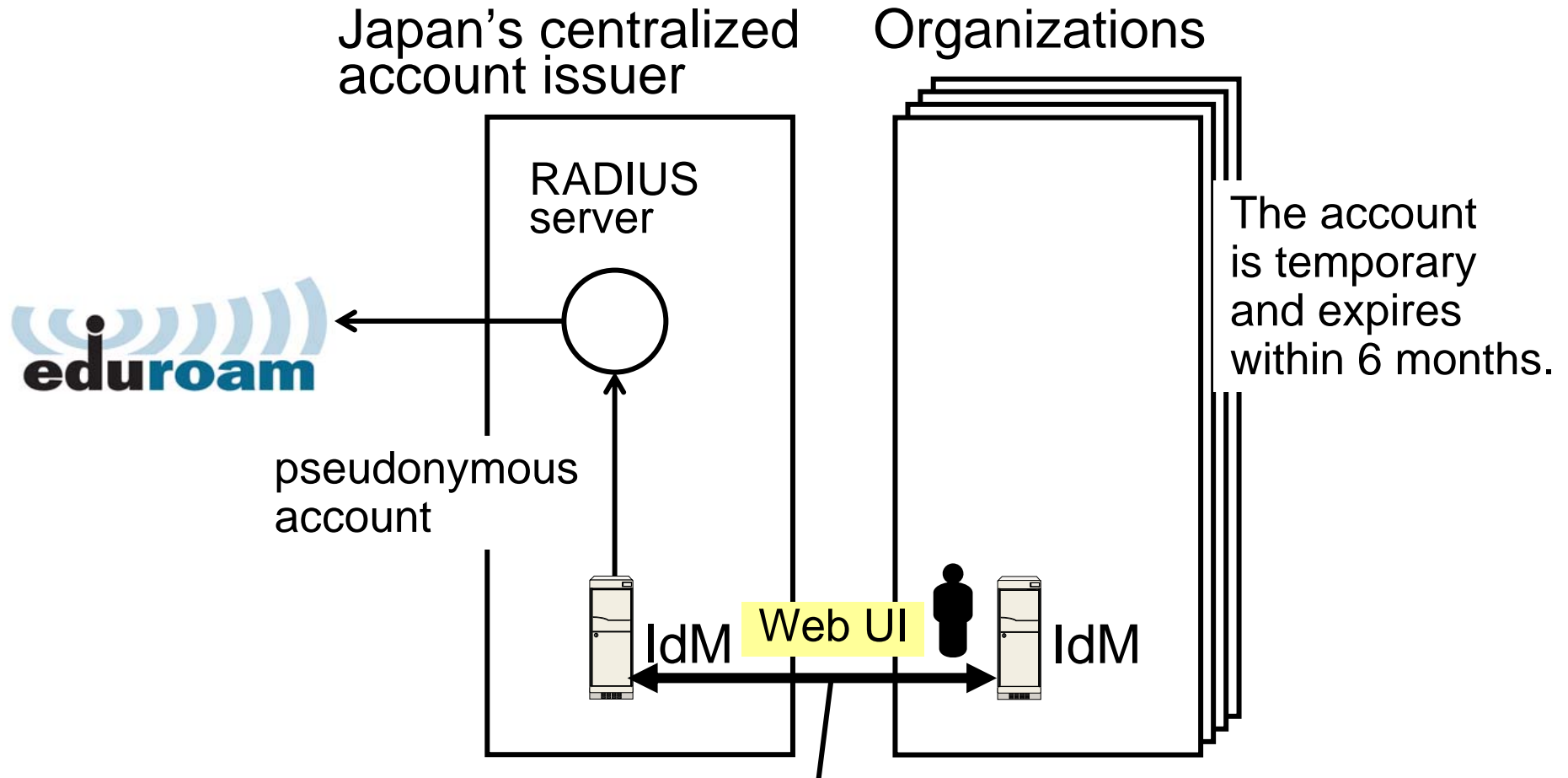
# Delegate Authentication System - Type I



Manual account issue requests by administrators.

- The system can be used even without IdM.
- Issuing Guest IDs is possible.

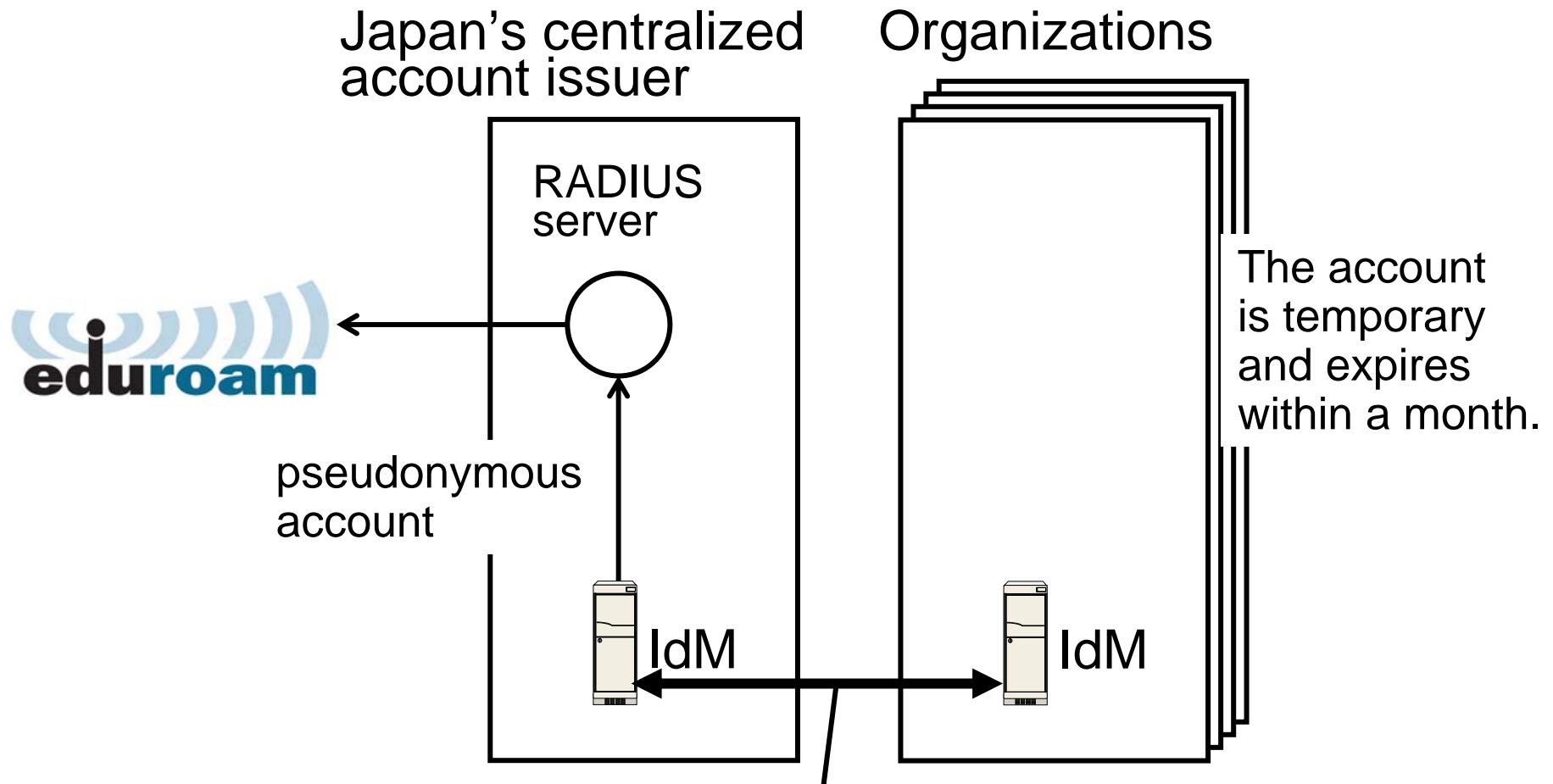
# Delegate Authentication System – Type II



ID federation using Shibboleth/SAML for administrators only.

- Administrators can request for user accounts in bulk.
- Issuing Guest IDs is possible.

# Delegate Authentication System – Type III



ID federation using Shibboleth/SAML

- End user can request for *personal accounts* only.



# RADIUS Semi-Open Proxy

## ■ The idea

- Open the *IP address and secret* of national RADIUS proxy to the public.
- Allow any organization (incl. convention centers and commercial ISPs) to connect APs to eduroam. (not IdP!)
- Accesses to the proxy server are restricted within .ac.jp and contracted ISPs.
- Universities do not need to contact the national administrator.

We will be able to promote eduroam AP deployment ! 10



# Security considerations

- What is the key used for?
  - To authenticate the client (authenticator) ?
    - (Raw) ID/PW are never provided from the national server.
    - No need for client authentication.
  - To authenticate the national server?
    - Yes. AP needs to know whether it is connected to the right server.
    - But...  
Can a stranger change the route to the national server when a wired and physically-secured network is used?
- Then, the key may be omitted, right?



## Security considerations (contd.)

- Is the authentication safe without the secret key?

- Yes.

- 802.1X authentication is safe against server spoofing or fake AP. Raw PW will not be revealed to the server.

- What about brute-force attack?

- The attack is possible through the APs even on the current system using the secret key.

- = key usage does not matter

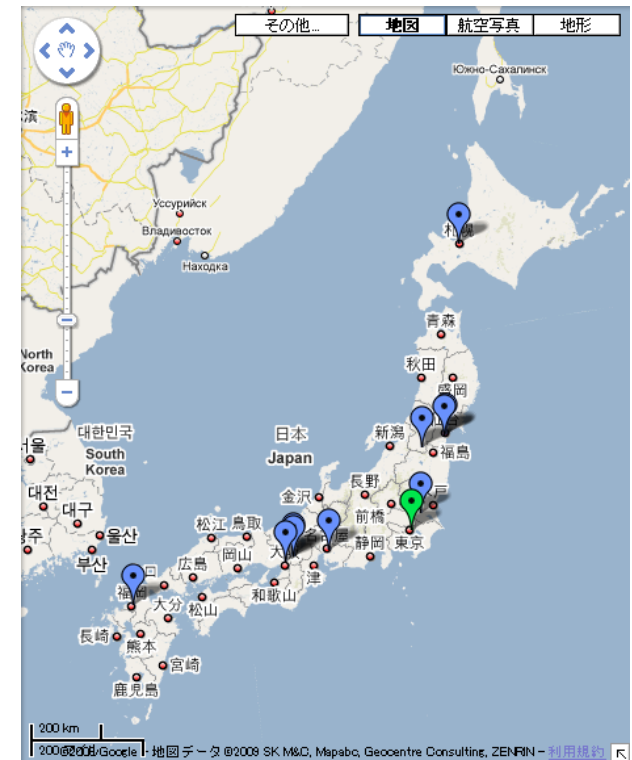
- Countermeasure should be implemented as a separate system (if it is needed).



# Supplementary slides

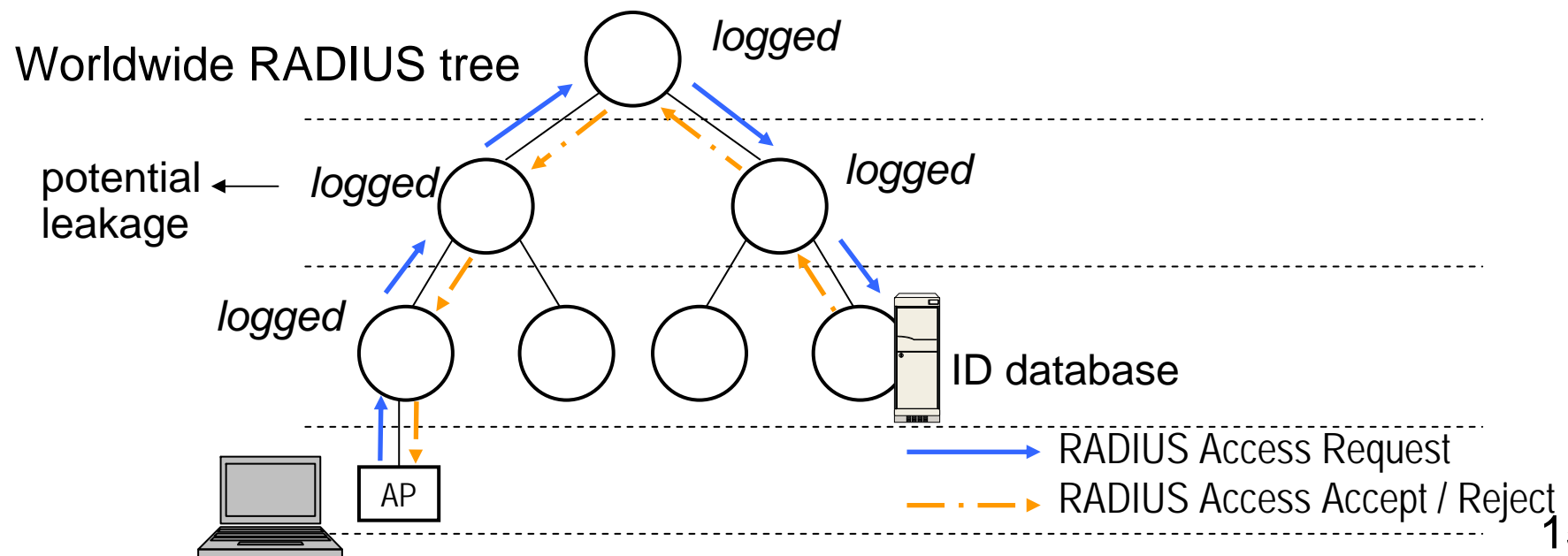
# eduroam JP in UPKI project

- An activity in NII's UPKI project
  - Promotion and operation of eduroam JP
  - 11 organizations connected (Oct. 2009)
  - Tutorial & technical documents
- R&D to solve problems
  - Large-scale deployment
  - Difficulties in configurations
  - Guest use of local IP addresses
  - Location privacy, etc.
- Talks with commercial W-ISPs for roaming
  - Shared access points possible?
  - ... *still seeking for a solution*



# Threats of ID/PW leakage

- User ID is logged at proxy servers along the AAA path.
  - Location privacy problem.
- PW could be logged due to inappropriate configuration by the user.
  - Critical security breach if an important PW is used.





## Pseudonymous account

- User can be *anonymous* in normal usage.
  - Admins of proxy servers outside the home organization cannot know (or guess) who exactly the user is.
  
- Malicious and/or harmful users can be tracked down in case of any incidents.
  - Better than using *fully-anonymous accounts* from administrative points of view.
  
- Can deal with *privacy protection laws* introduced in some countries ?