July 11, 2025
COMPSAC/SAPSE2025 Workshop, Toronto

Offline Attribute Sharing Methods for Authentication Traffic Reduction and Functionality Enhancement of Wireless LAN Roaming Systems

Hideaki Goto　Tohoku University

Part of this work was supported by JSPS KAKENHI Grant Number JP25K03103.

Secure Wireless LAN Roaming

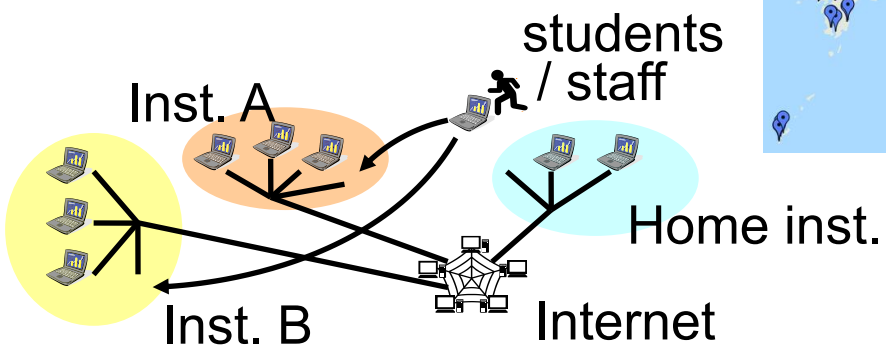
- Wi-Fi roaming systems allow users to join wireless networks at various places even across different operators.
- No need for cumbersome sign-up.

eduroam

for Research&Education (2002-)

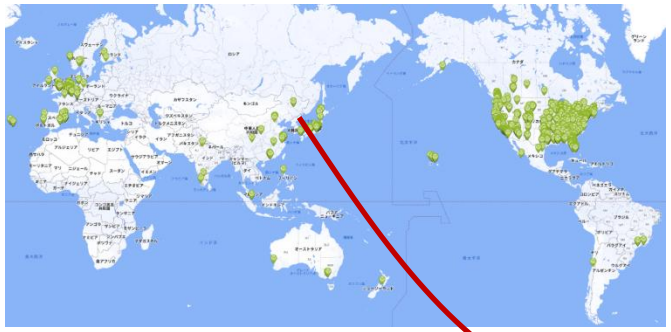
104 countries / territories

eduroam JP

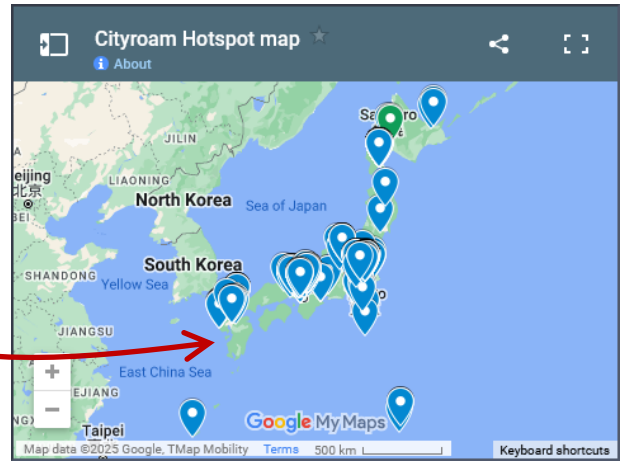


OPENROAMING™
WIRELESS BROADBAND ALLIANCE

for Everyone (2020-)



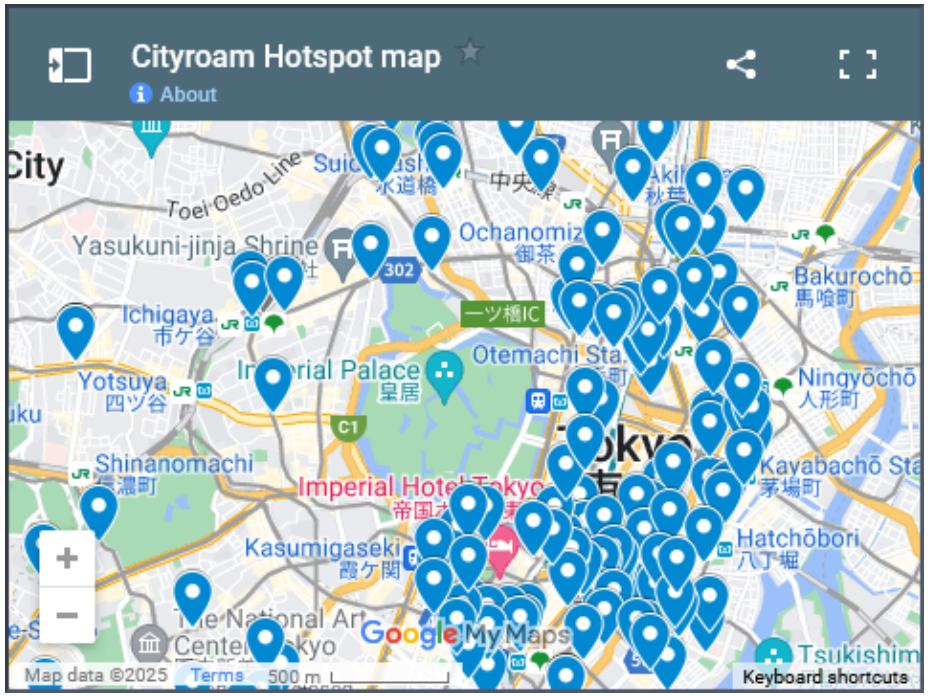
cityroam



1000+ spots (July 2025)
eduroam is combined.

TOKYO FREE Wi-Fi supports OpenRoaming

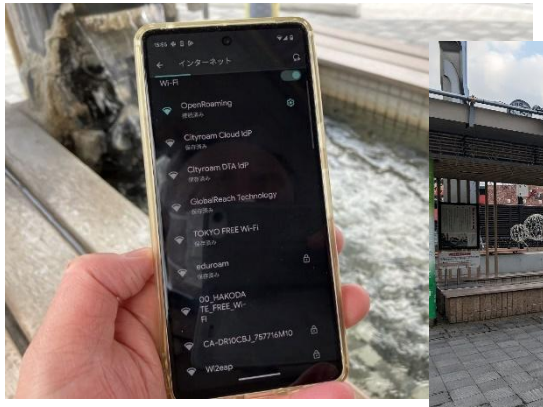
- Released on Mar. 31, 2023
- Tokyo Metropolitan Government + KDDI / Wire & Wireless (Wi2)
- Enhanced security, safety, and usability. ☺

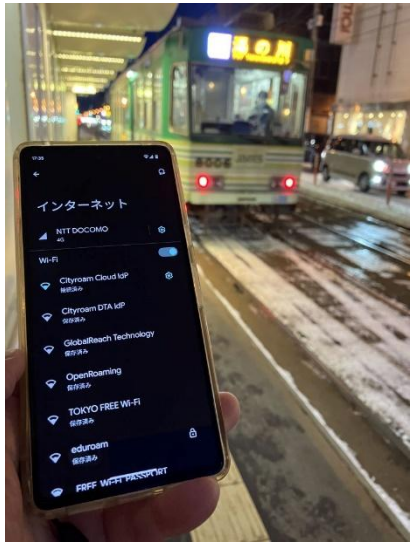


https://wi-fi.metro.tokyo.lg.jp/en/

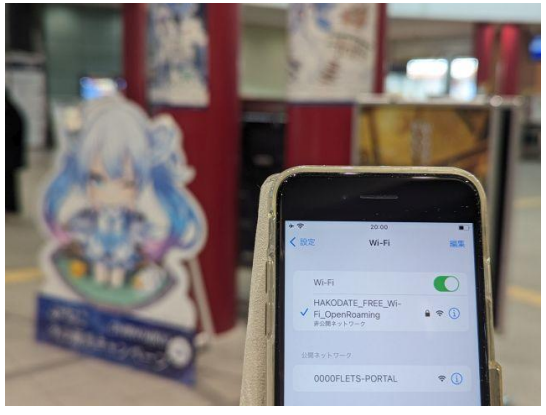
HAKODATE FREE Wi-Fi

- Nov. 30, 2023 –
- eduroam and OpenRoaming become available.





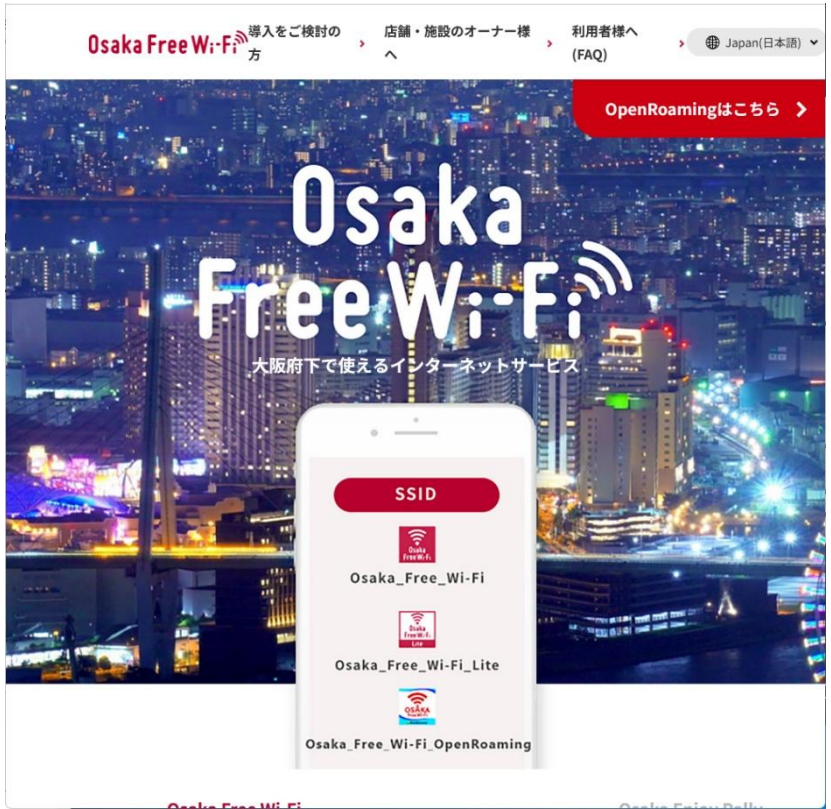
Enjoy eduroam / OpenRoaming
at the footbath (hot spa), airport, trams !



https://wi2.co.jp/release/press/2023/20231130-hakodate_openroaming.html

Osaka Free Wi-Fi

- Oct. 10, 2024 –
- Initial deployment focuses on Public Transport. (for EXPO 2025)

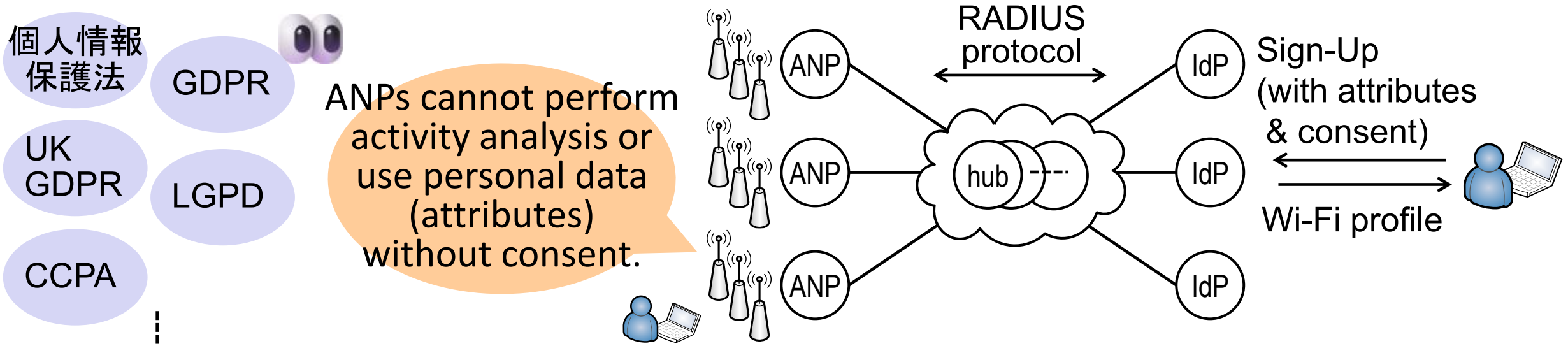


OSAKA Free Wi-Fi
Open Roaming

https://ofw-oer.com/

Challenges in user activity analysis and data usage

- IdP and ANP are separated.
- **ANPs cannot see “real user ID” or obtain user’s consent.**
  - Outer-Identity is anonymized, e.g. anonymous@example.com
    Inner-Identity is protected by **EAP tunnel** between User Device - IdP.
  - EAP-TLS (with TLS 1.3) hides the contents of Client Certificate.
  - Ephemeral MAC addresses, etc.



ANP: Access Network Provider
EAP: Extensible Authentication Protocol

Problems, and Research Objectives

- Lack of standard framework for attribute/consent sharing imposes **significant impact to the business model,** introducing a great hurdle in deploying Wi-Fi Roaming.
- Roaming systems suffer from a large number of **invalid authentication requests** from devices with expired or revoked credentials.

Objectives

- Explore some methods for sharing attributes/consent in an *offline manner*.
- Address the high load problem.
- Prepare for some prospective use cases, including *disruption-tolerant Wi-Fi roaming systems*.

Development of a user data sharing system

- Owners want to know / do …
  - Age group
  - Gender
  - Nationality
  - Language (browser setting)
  - Device/OS (for app development)
  - Wi-Fi usage location and staying time
  - Travel routes (e.g. shop-hopping in a mall, tourist sites), etc.

- Especially, municipalities want to know / do …
  - Travel routes
  - Analysis of tourist sites
  - Analysis for disaster response / mitigation, and urban design

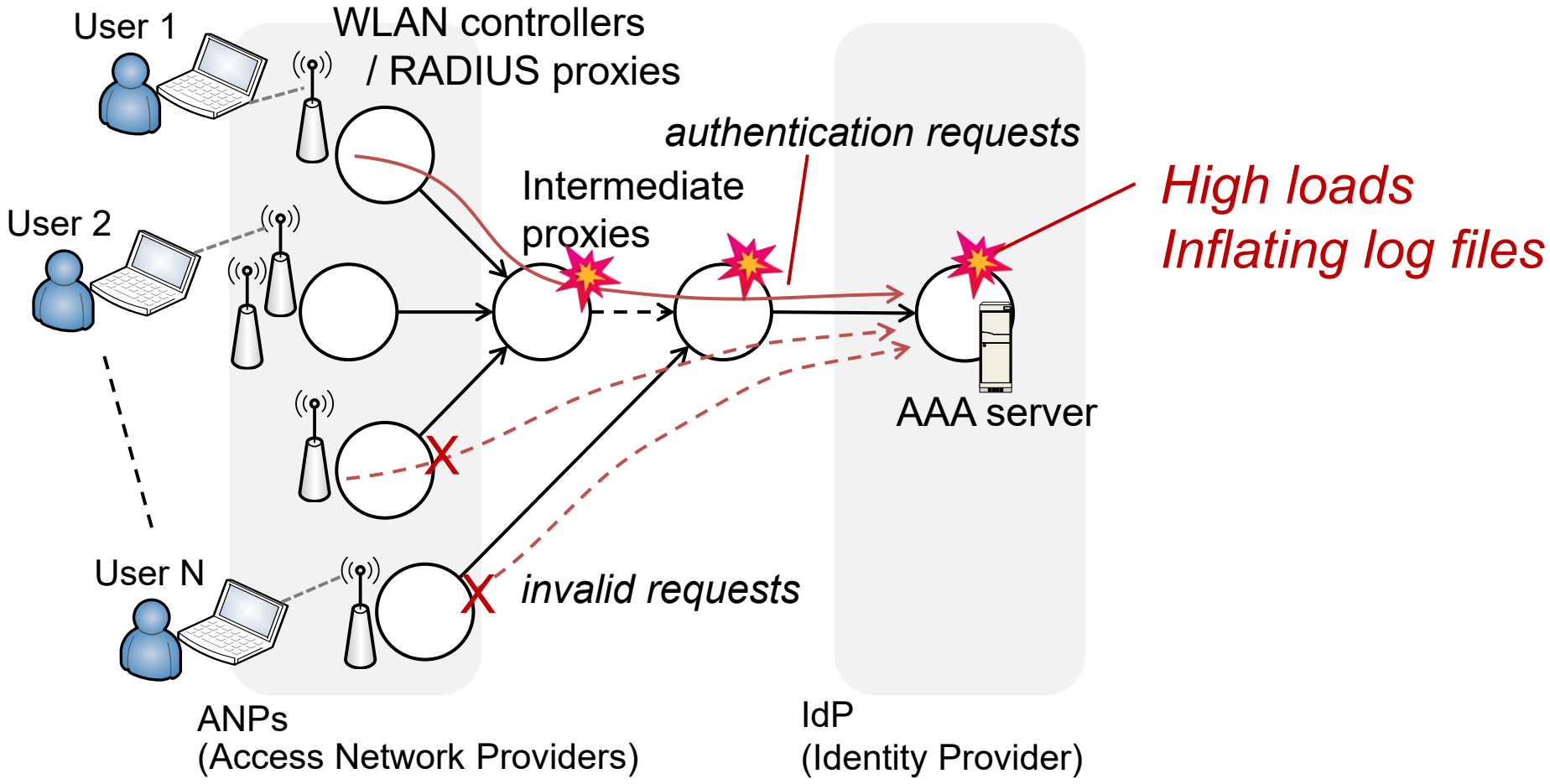
Three methods

1. Embed Valid Until date in the RADIUS User-Name.
   - Suppress invalid authentication requests.
   - Can be forged, but with no significant impact.

2. Embed simple attributes in the User-Name securely.
   - Suitable for public attribute sharing.
   - Tamper-resistant.

3. Per-group attribute sharing using Local Authentication and ECDH
   - Generalized, group-based attribute sharing.
   - Tamper-resistant.
   - Realize User Activity Analysis and Personal Data Usage even in roaming systems.

1. Reducing invalid requests caused by expired/revoked credentials



1. Reducing invalid requests caused by expired/revoked credentials

Solution

Embed Valid Until data in the User-Name so that ANPs can see it and stop invalid requests.

anonymous@**vu250331**.example.com

(realm part)

Why in the realm part? – ANPs can see only Outer-Identity.
User ID is often anonymized.

User can modify it ! – AAA server knows real date. ☺

In 2023, our multi-tenant eduroam IdP service saw:

9.6% expired credentials, (= max reduction rate)

20.4% AuthN failure log lines

2. Tamper-resistant attribute sharing method with *Local Authentication*

(H. Goto, JIP 2024)

Solution

Embedding attributes and digital signature.

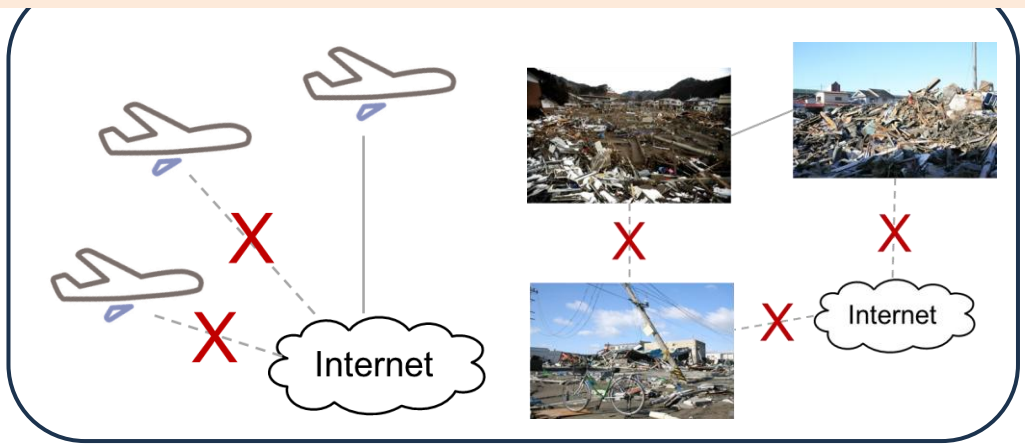
CYEPBcv7T|MCUCEQC3SwoCbmNfPno3KRv
ZP7qLAhBg+cHjunGEo6CwKPzHeNz7@**xattrjez**
tqpof52n2xxm7vphkeocp5aqbil43.example.com

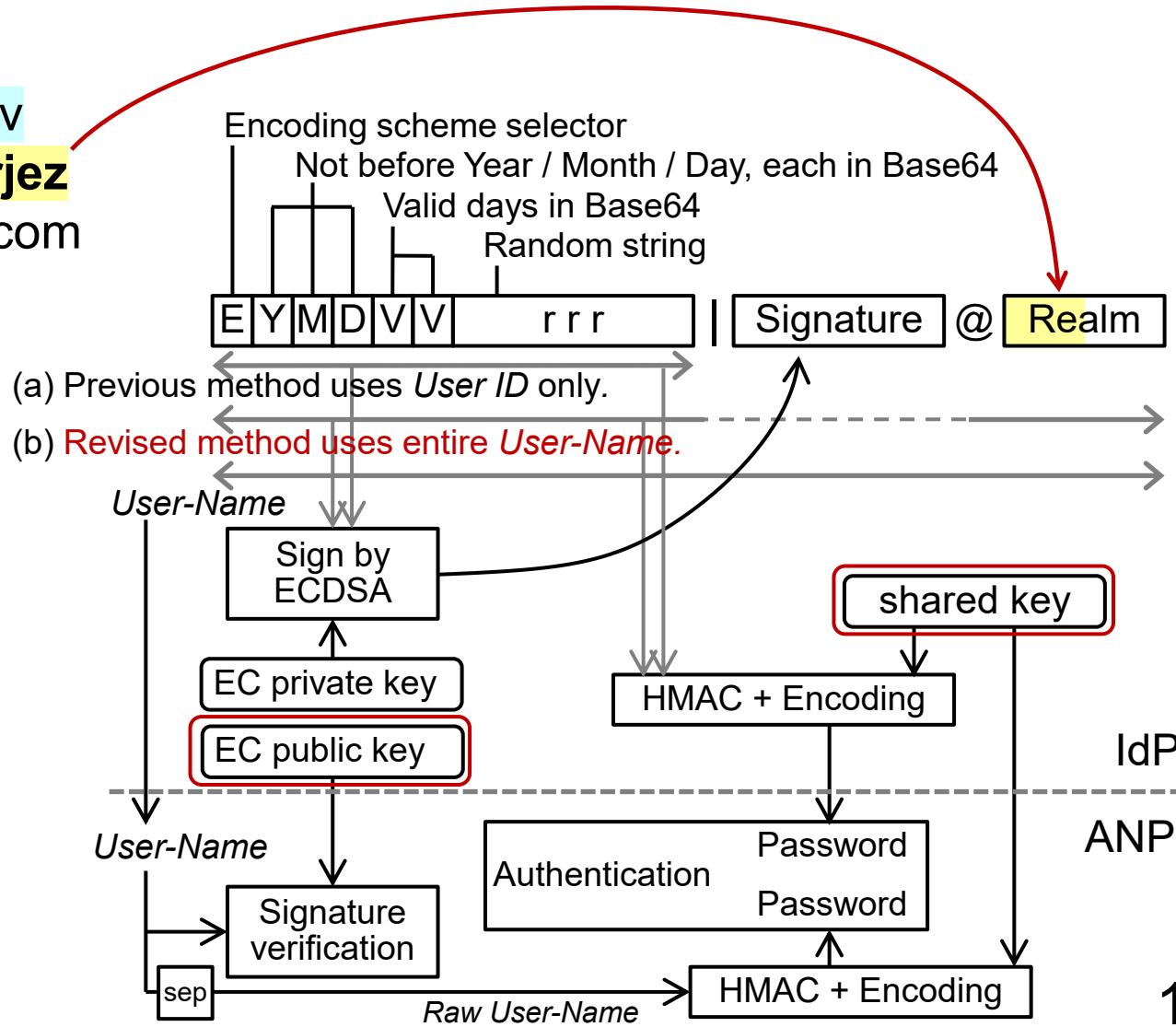
Use regex for realm-based routing.

realm "~^(.+\.)?example\.com$“ { … }

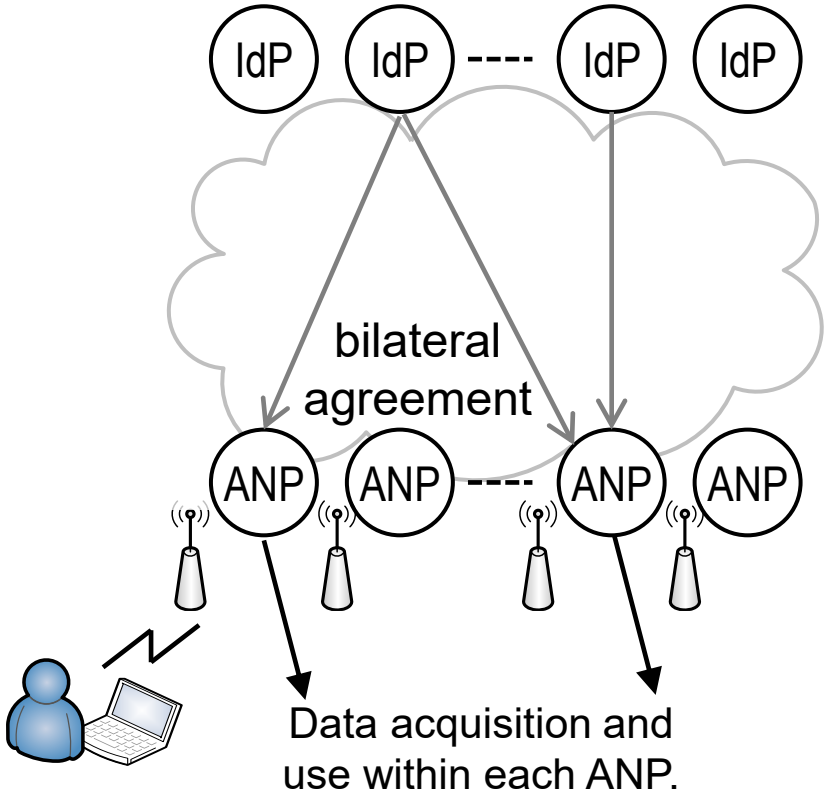
Prospective use cases:

In-Flight Wi-Fi, and Public Wi-Fi in disaster-affected areas

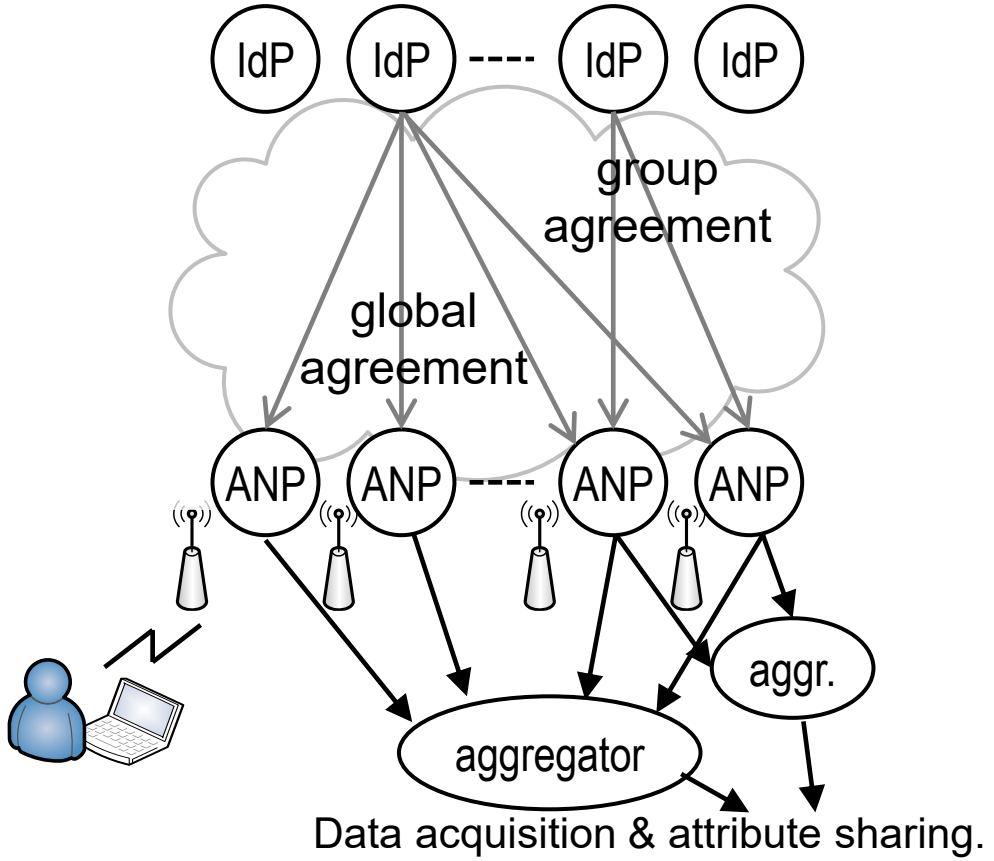




3. Per-group attribute sharing using Local Authentication and ECDH



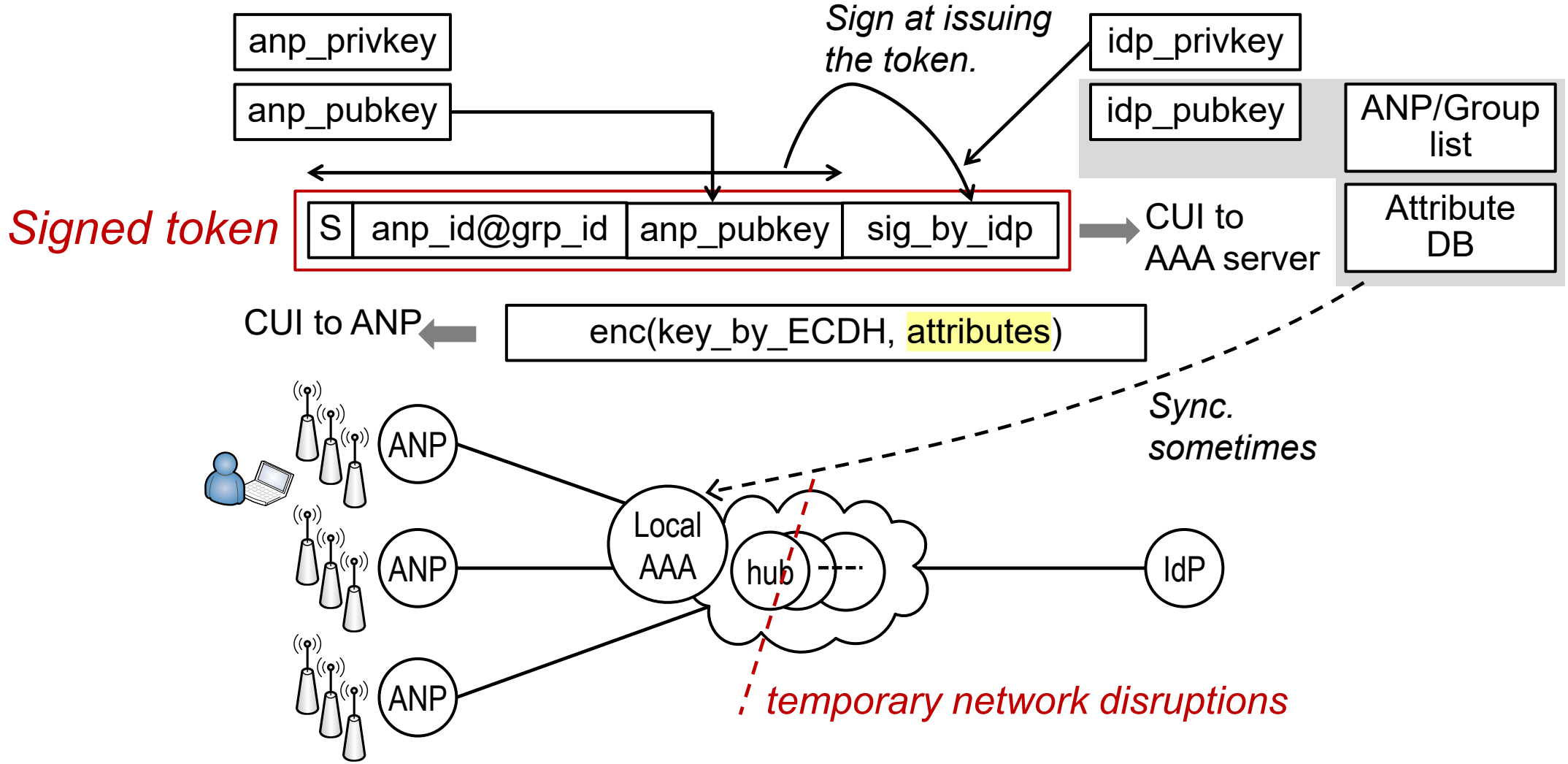
(a) Conventional roaming system based on bilateral agreements.



(b) Roaming system with global / per-group attribute sharing.

3. Per-group attribute sharing using Local Authentication and ECDH

- Use RADIUS protocol to deliver attributes.
- Support occasional changes of user attributes.

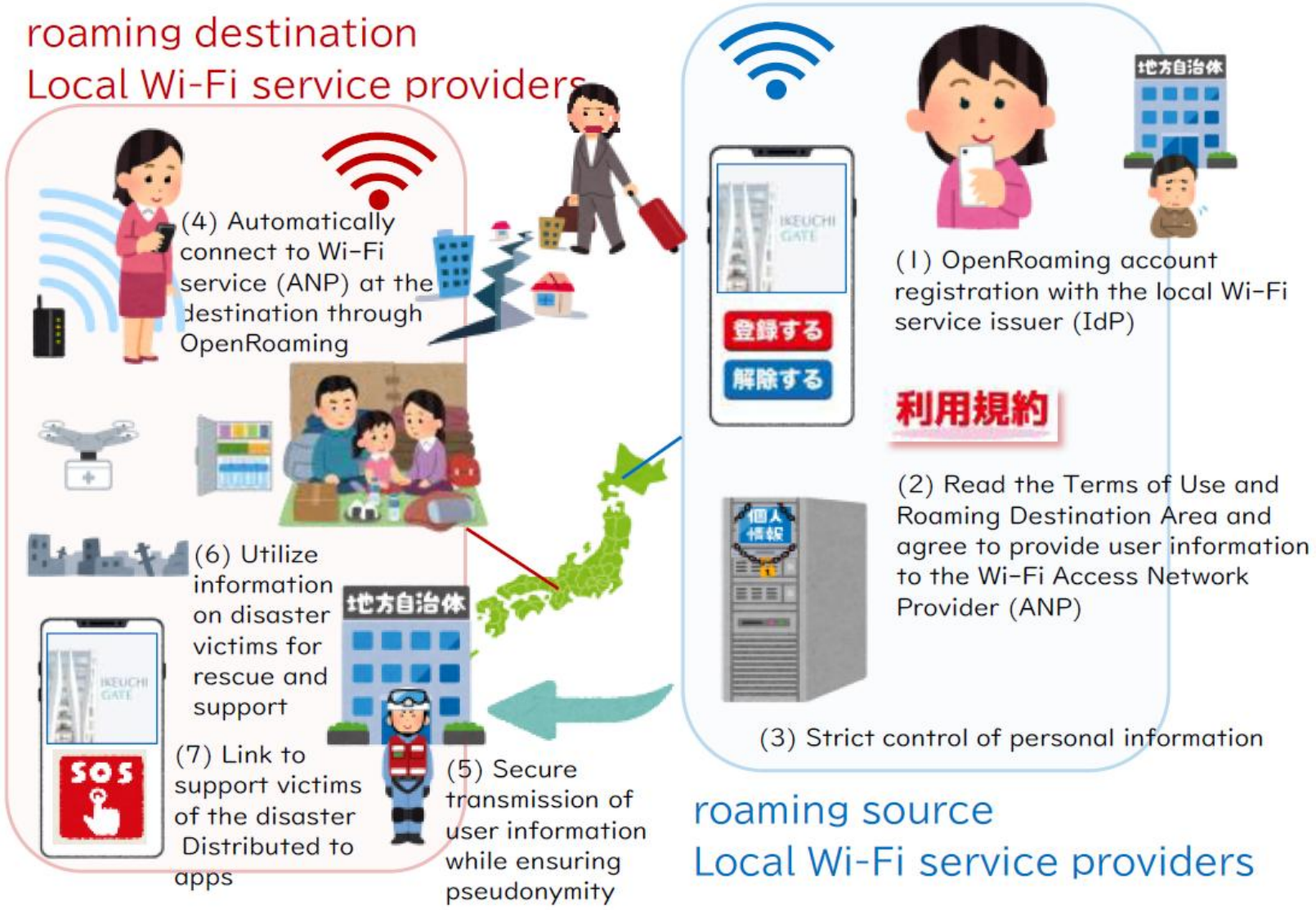


Use case 1: Regional tourism apps

Y. Okabe et al.,
IPSJ CDS43, 2025

Commissioned research 23610 by National Institute of Information and Communications Technology (NICT), Japan (2024-2025)

Use case 2: User search and support under natural disasters



Commissioned research 23610 by National Institute of Information and Communications Technology (NICT), Japan (2024-2025)

Conclusions

Developed three methods for attribute sharing.

1. Embed Valid Until date in the RADIUS User-Name.
   - Reduce invalid authentication requests.
2. Embed simple attributes in the User-Name securely.
3. Per-group attribute sharing using Local Authentication and ECDH
   - Generalized, group-based attribute sharing.
   - Tamper-resistant.
   - Realize User Activity Analysis and Personal Data Usage.

Future work

- Develop attribute/location-based services for roaming systems.
- Business model development and analysis.