COMPSAC SDIM2022 Workshop (Virtual)
27 June – 1 July, 2022

Disruption-tolerant Local Authentication Method for Continuous and Secure In-Flight Wireless LAN

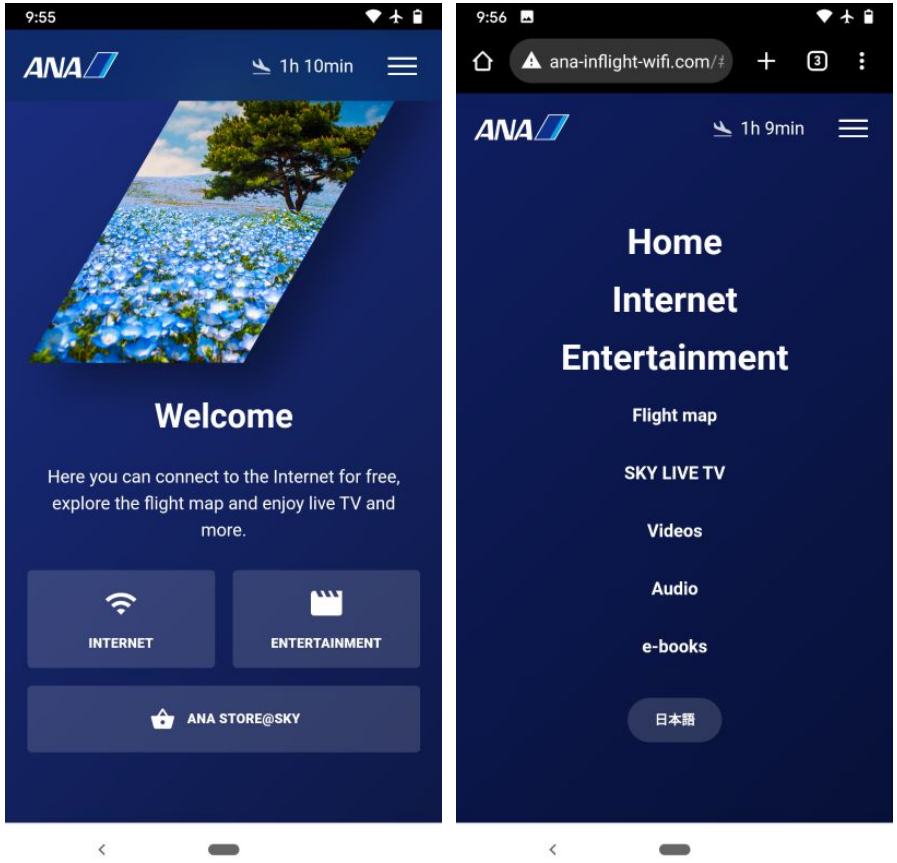
Hideaki Goto
Tohoku University, Japan

(Supported in part by JSPS KAKENHI No.19H04090)

Evolving In-Flight Wi-Fi service

- *Internet connection* used to be the main application of In-Flight Wi-Fi many years ago.
- Now, In-Flight Wi-Fi provides a wide range of services including:
  - internet connection
  - flight map/information
  - venue information
  - audio/video streaming using onboard media server
  - shopping

In-Flight Wi-Fi is becoming an indispensable service, especially in longhaul flights.



Problems in current In-Flight Wi-Fi service

- Lack of security due to “open network”.
  - Evil-Twin APs.
  - Man-in-the-Middle (MITM) attacks, etc.
- Low usability (manual Wi-Fi configuration).
  - Find the right SSID,
  - figure out how to connect, (& troubleshooting,)
  - read Terms of Service,
  - and type in ID/password for paid service.
- Disruption of internet connection.

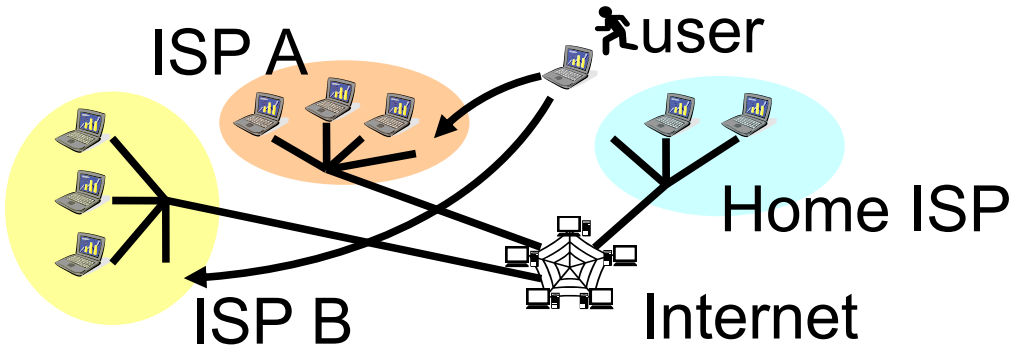
Wi-Fi industry has been working on these problems.

OpenRoaming will provide secure, seamless and automatic connection means.

OPENROAMING™
WIRELESS BROADBAND ALLIANCE

Introducing a secure Wi-Fi roaming

- WPA2/WPA3 Enterprise can solve the security problems, allowing users to “roam” securely between different ISPs.
- RADIUS servers are used to deliver the access requests from user devices to users’ home IdPs (Identity Providers).
- The current roaming systems in In-Flight Wi-Fi, based on open network (unsecure), will be upgraded.
  Wi-Fi roaming using phones’ SIM cards will be available.
- Network disruption is still a great problem.
  User authentication is dependent on the authentication server on the ground.



Research Objectives

- Sort out prospective use cases and problems of future In-Flight Wi-Fi with roaming capability.

- Develop **user authentication and roaming system tolerant of network disruption** in order to realize continuous and secure In-Flight Wi-Fi service.

User journey with current In-Flight Wi-Fi

Boarding

You are requested to turn off the cellular.

You have to manually configure Wi-Fi.

No internet connection. (local contents only)

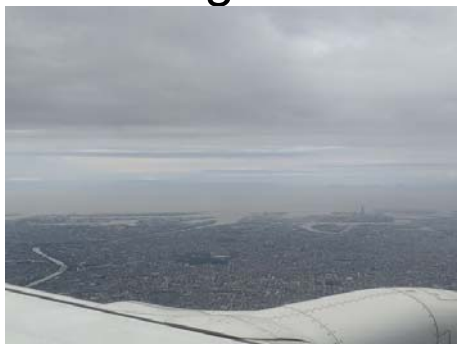
Taxi & Take-off

Reach 10,000 ft.

Internet connection is turned on.

Some disruptions may occur inevitably.

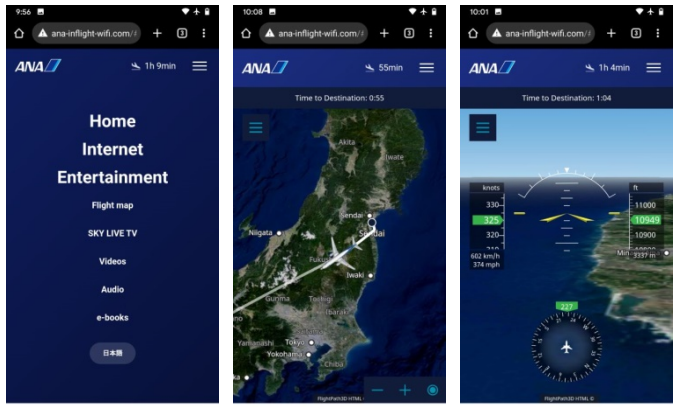
Landing



Internet connection is turned off.

In a foreign country, you would lose network until you buy a SIM card.

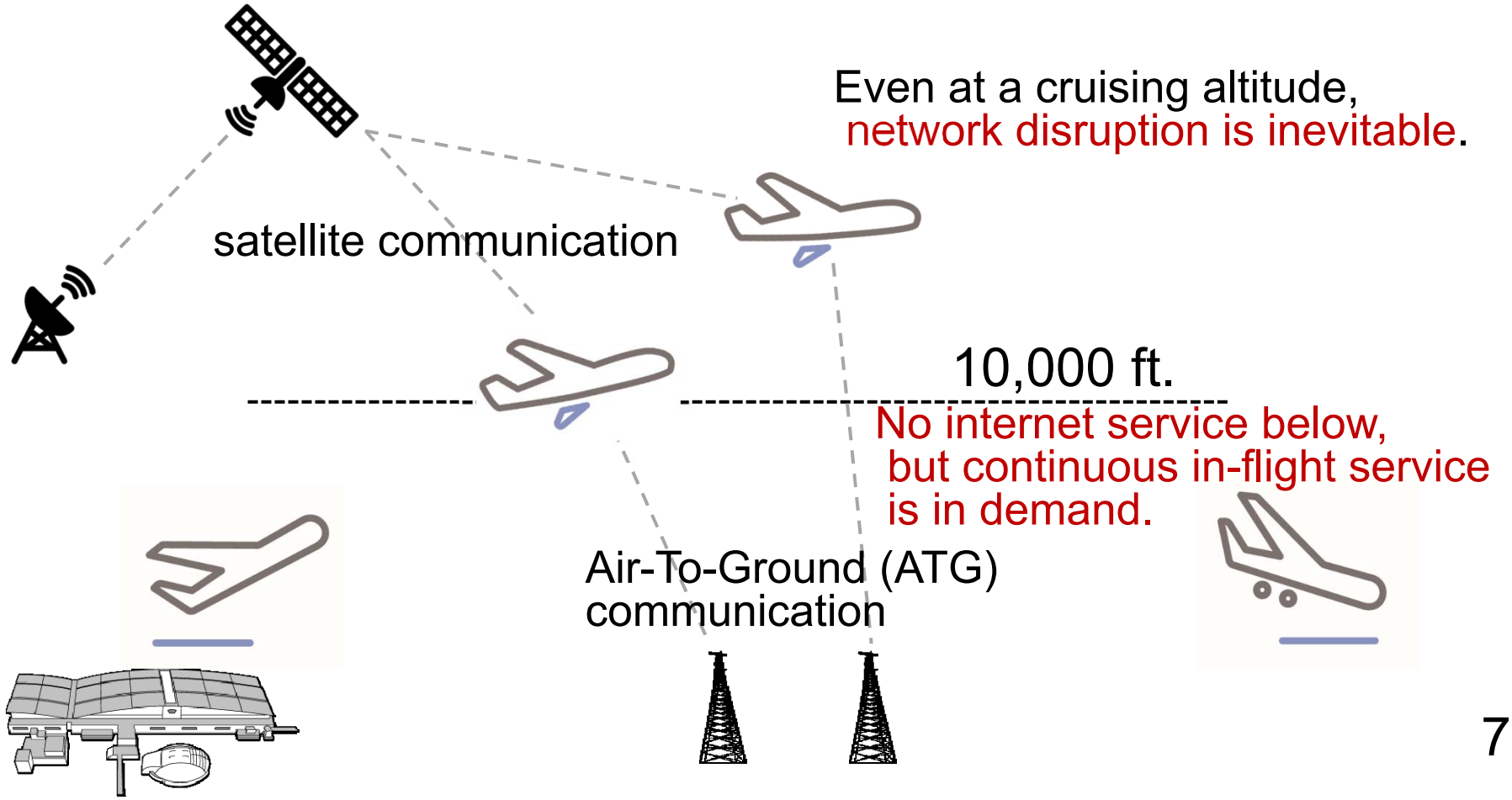
Cruising



You enjoy various local contents & the internet.

In-Flight Wi-Fi and backhaul network

- Satellite & ATG networks are evolving, but network disruption is inevitable. (weather cond., regulations, etc.)
- We want to avoid interruption of *in-flight services* such as audio/video streaming, shopping, etc.



In-Flight Wi-Fi with roaming

Roaming is supposed to improve *security and usability*, but…

Pros

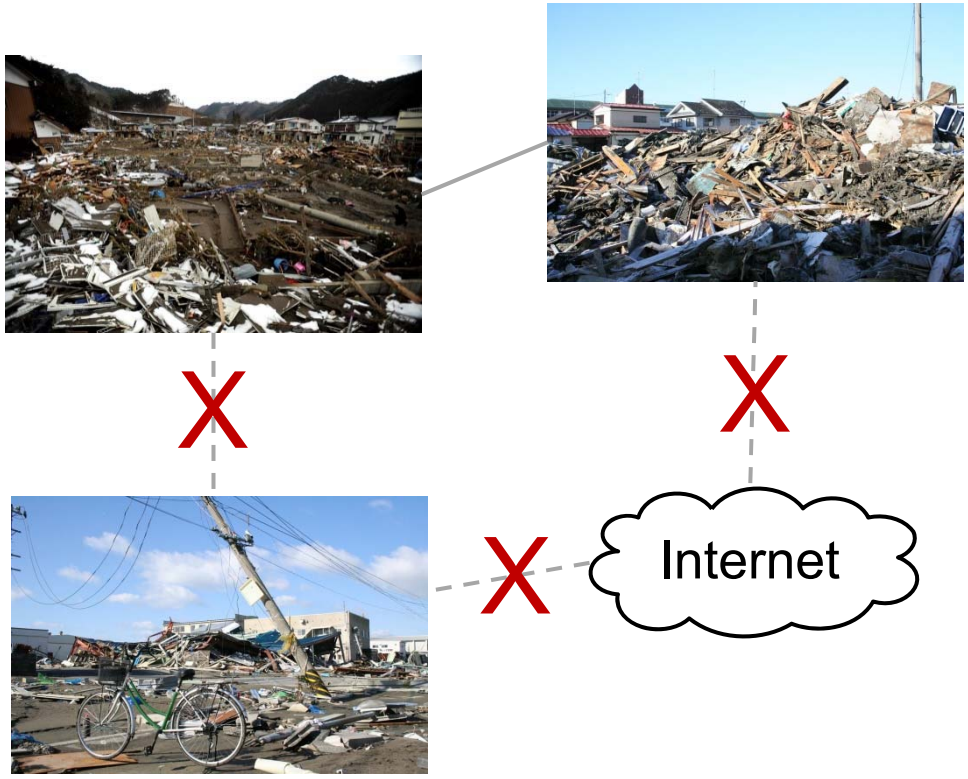
- Roaming involves user authentication.
- Per-user encryption of wireless communication can be achieved by 802.1x-based user authentication.
- Airlines and ISPs can provide better network service to those who pay more.

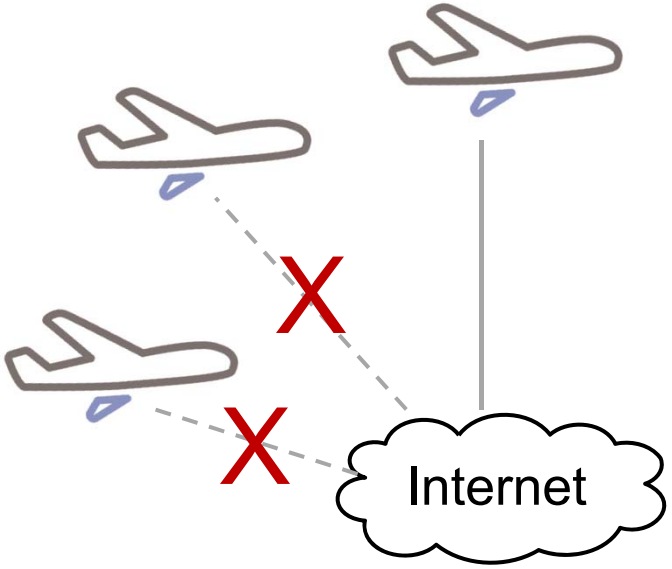
Cons

- User authentication does not work during network disruption. Passengers are unable to use local services.
- Local services may be interrupted when the “re-authentication” of 802.1x runs and fails during network disruptions.

Similarity with the use case in natural disasters

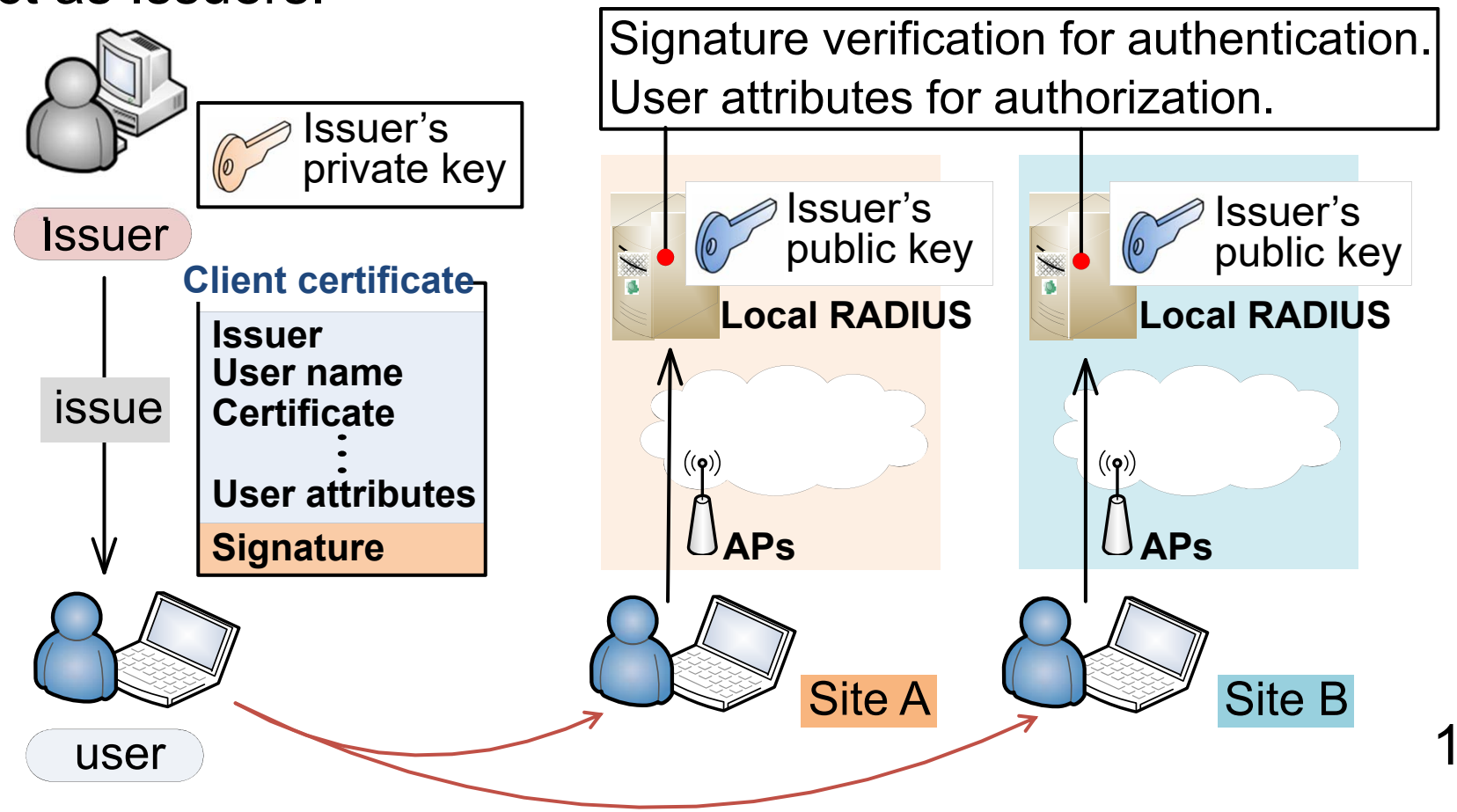
- Disaster-affected areas may suffer from *communication isolation* due to the disruption of the backhaul network.
- People want to use public Wi-Fi even on a local network.
- But, the public Wi-Fi cannot be used since the user authentication is dependent on a remote server.





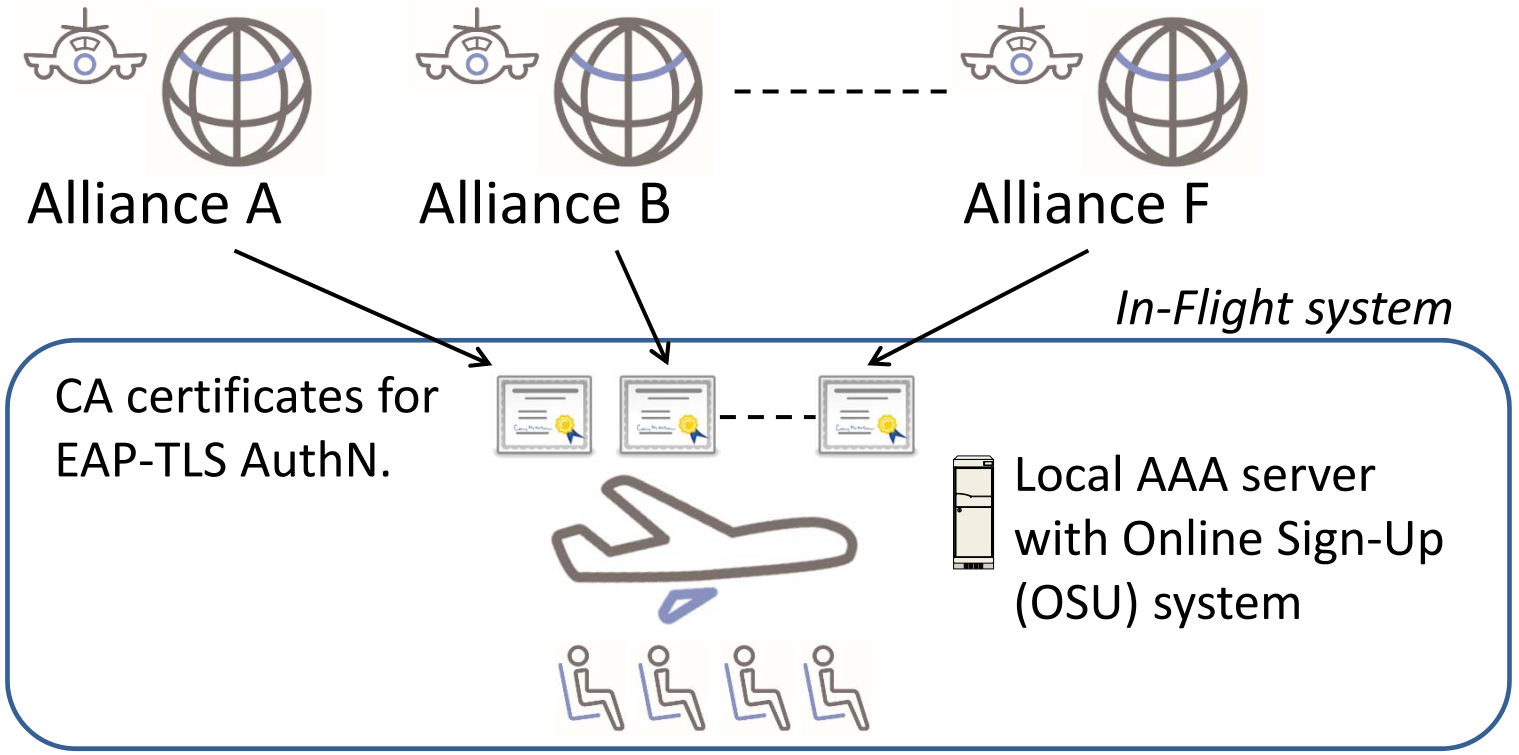
Certificate-based local authentication

- Originally developed for disaster- and disruption-tolerant Wi-Fi system for disaster-affected areas. (COMPSAC 2013)
- Local user (client) authentication is realized by EAP-TLS.
- For scalability, 47 prefectures in Japan were supposed to act as Issuers.



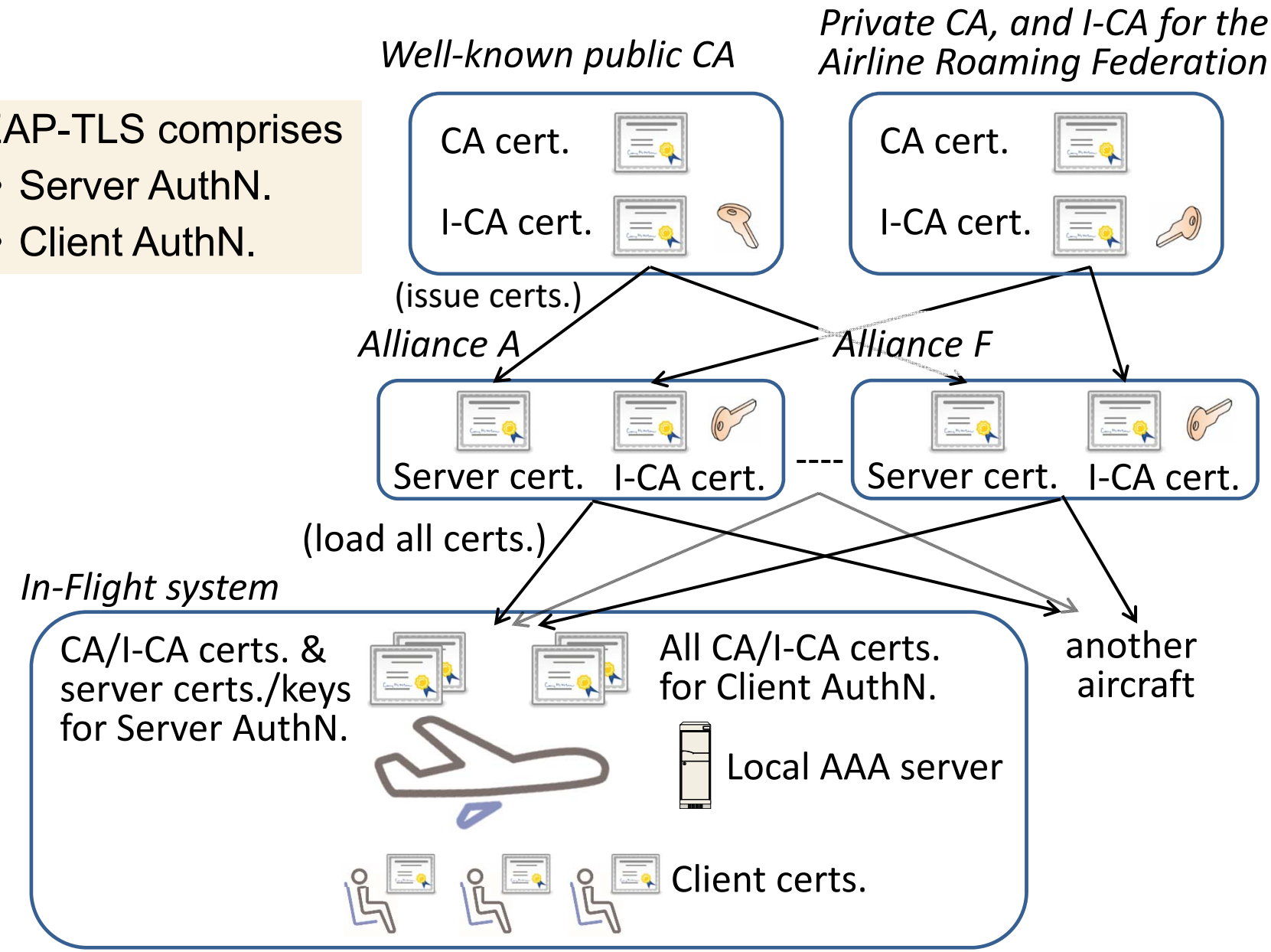
Local authentication for In-Flight Wi-Fi

- A limited number of operator groups, such as airline alliances, provide CA certificates and issue client certificates.
- A challenge exists in secure operation and handling of the CA certificates as many aircrafts are carrying them.



Certificate chains

EAP-TLS comprises
- Server AuthN.
- Client AuthN.



Public CA or Private CA?

Server authentication phase:

- It is technically possible to install a CA certificate together with a client certificate on user devices.
  Adding CA certificates frequently is not so safe.
- User devices have built-in CA certificates from many public CAs.
  We prefer public CA to ease device configuration, avoiding complexities.

Client authentication phase:

- We should use private CA.
  If a public CA were used, an attacker would obtain a client certificate from the same CA and enforce the client authentication to succeed.

Wi-Fi profile issuing and roaming

In-Flight Wi-Fi needs to provide various means for passengers to obtain a profile *electronically*.

- Users download a profile at airline websites upon reservation.
- Airline app automatically downloads a profile and configures the user device.
- Unprepared passengers use Online Sign-Up (OSU) system onboard an aircraft.
  - Local profiles without roaming capability may be issued.
  - User verification without internet connection is a challenge.
- Users receive or buy a voucher and use the OSU.

Passengers may use connection flights.

If the airlines are participating in the federation, roaming is possible even between different airlines.

Security considerations

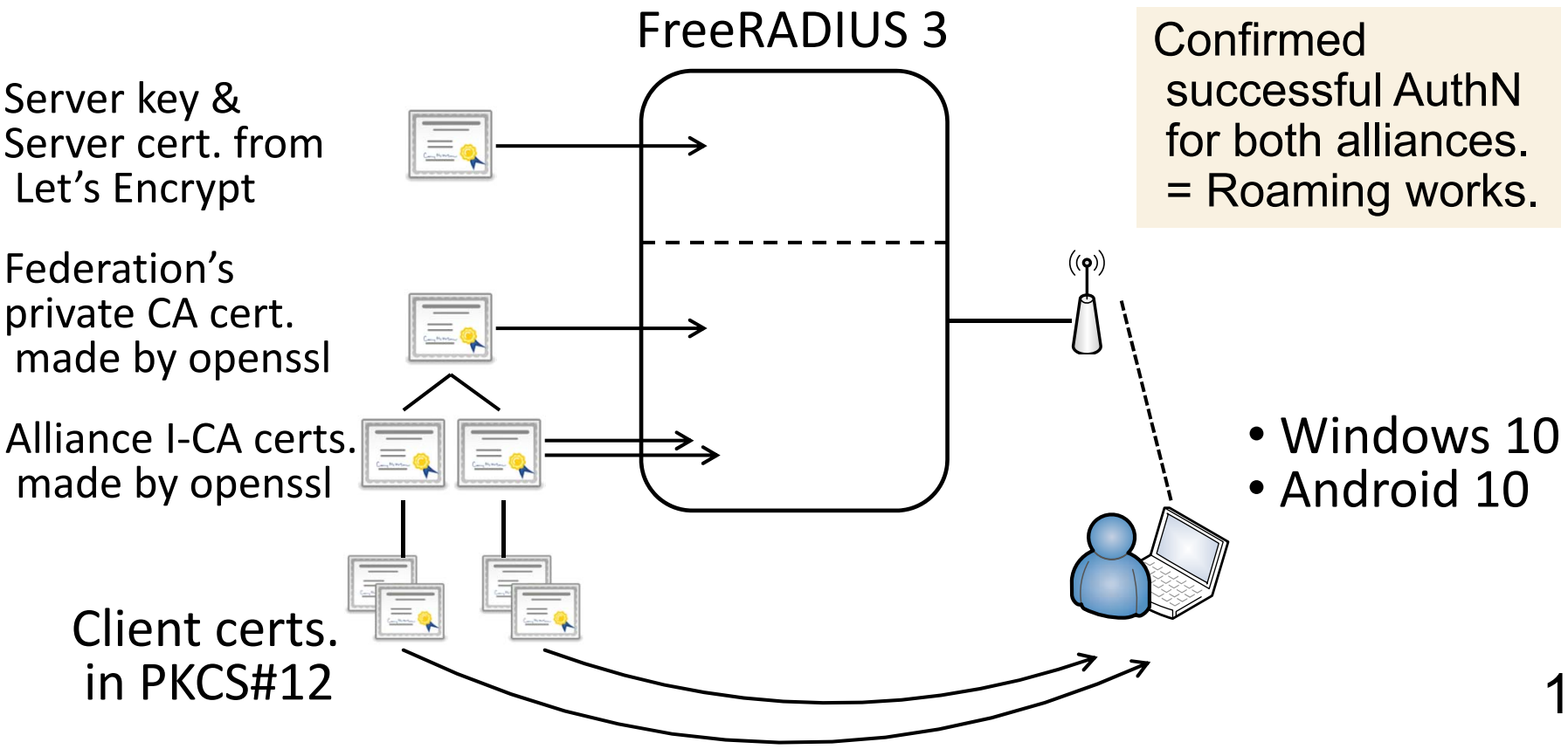
Leakage of CA/I-CA certificates leads to security risks.

- Use of CRLs is difficult, although a caching mechanism would be useful.
- Shorter lifetime of I-CA certificates is preferred to mitigate the impact from potential certificate/key leakage.
  (e.g. 90 days in Let's Encrypt)

- Lifetime of client certificates is affected.
  Automatic certificate renewal will help users keep Wi-Fi profile always updated.
  Development of a PoC app is under way.

PoC system and functionality tests

- We developed a Proof-of-Concept roaming system.
  - 2 virtual alliances.
  - Server certificate issued by Let's Encrypt.
  - openssl command for certificate issuing.



Summary

- We have analyzed some prospective use cases of In-Flight Wi-Fi and technical challenges.
- We have developed a *disruption-tolerant user authentication method* for realizing continuous and secure In-Flight Wi-Fi.
  - Roaming is possible, accepting user credentials from some operator groups (alliances).
  - The roaming system is based on the popular EAP-TLS. It would be easy to combine it with other systems.
- We have built a Proof-of-Concept system and confirmed that the developed framework works well as designed.

Future work

- Develop an app for automatic profile handling.
- Develop a method for profile association with telco/ISP ones.