A Privacy-Preserving Architecture for Location-Aware Services in Inter-Regional Public WLAN Roaming

Yasuo Okabe
Academic Center for Computing and Media Studies
Kyoto University
Kyoto, Japan
okabe@i.kyoto-u.ac.jp

Takenori Hirose
Local 24, Inc.
Kyoto, Japan
hirose@local24.jp

Ayaka Kurosawa
Local 24, Inc.
Kyoto, Japan
kurosawa@local24.jp

Eisaku Sakane
National Institute of Informatics
Tokyo, Japan
sakane@nii.ac.jp

Hideaki Goto
Cyberscience Center
Tohoku University
Sendai, Japan
hgoto@cc.tohoku.ac.jp

***Abstract*— In RADIUS-based public Wi-Fi roaming services such as eduroam and OpenRoaming, users are identified using a temporary pseudonym called CUI (Chargeable User Identity) issued by the IdP. Neither the IdP nor the ANP (Access Network Provider) can independently determine "who is where", which structurally ensures location privacy. However, due to this structure, even when users consent, providing location-aware services while identifying the user remains challenging. In this paper, we propose a new architecture that separates the IdP, ANP, and LB (Location Broker) into three distinct entities. The IdP generates a CUI by combining the real ID and a pseudo ID but does not know the location. The ANP holds the location and CUI but does not know the real ID nor the pseudo ID. Only the neutral LB combines the pseudo ID and location information for sessions with explicit user consent and securely supplies it to LSPs (Location-aware Service Providers). By strictly limiting the entity responsible for binding real IDs and location information, this architecture demonstrates the ability to maintain location privacy while providing location-aware services resistant to location spoofing. We will also discuss business use cases for inter-regional collaboration utilizing this architecture, such as its application to tourism promotion and its use in evacuation shelters during disasters.**

Keywords*— *RADIUS, OpenRoaming, location-aware service, location privacy, pseudonimity

I. Introduction

In roaming systems based on IEEE 802.1X + RADIUS such as eduroam [1] and OpenRoaming [2], the Identity Provider (IdP) issues a short-lived pseudonym, called the Chargeable User Identity (CUI), that links a session to a user without revealing the user's real identity to the Access Network Provider (ANP). Conversely, the IdP does not receive the user's location. This split achieves accountable anonymity: either party can help identify the user when strictly necessary, yet neither can unilaterally learn both identity and location. The separation, however, makes it inherently difficult, despite user consent, to deliver services that require simultaneously knowing who the user is and where they are.

Several consent-based schemes have been considered to add location awareness without sacrificing privacy, but each has significant drawbacks. One is RADIUS attribute approach. Location information can be attached to RADIUS packets (e.g., via RFC 5580 [3]) and forwarded to the IdP, yet only for users who have given prior consent. Doing so would require a new policy channel from the IdP back to the ANP, and—where the IdP is the user's home organization, as in eduroam—may be inappropriate because the university would learn its members' off-campus whereabouts. Another is based on an App-centered location broker. A client app collects GPS or Wi-Fi fingerprints and, at times chosen by the user, sends them under a pseudonym to an independent broker that merges identity and location under explicit consent. Although this keeps the IdP and ANP blind, any solution that relies on client-side sensing is vulnerable to location spoofing, enabling fraud and incentive manipulation.

This study exploits a key property of RADIUS-based Wi-Fi roaming: once an IEEE 802.1X session is established, the access point (whose physical location is known) serves as a trustworthy location proof that can be validated across the roaming federation. Leveraging this anti-spoof feature, we propose a three-party location-sharing architecture that inserts a neutral Location Broker (LB) between the Identity Provider (IdP) and the Access Network Provider (ANP). The IdP authenticates the user and issues a session-specific CUI, yet never sees location data. The ANP records the CUI together with the access-point location, yet never learns the real identity. Only the LB—after explicit user consent—may fuse the pseudonymous CUI with the recorded location. By keeping real identity and location under separate control and allowing their fusion solely within the LB, the scheme preserves location privacy while offering users verifiable, spoof-resistant location proofs for the limited scope they approve.

In Section 2, we describe the basic concepts and related research. In Section 3, we propose a RADIUS-based location information sharing mechanism involving three parties: IdP, ANP, and a location information broker. In Section 4, we discuss business use cases for this mechanism, including its application to tourism promotion and its use in evacuation shelters during disasters.

II. Basic Concepts

A. User Identification in RADUIS-Based Authentication

In IEEE 802.1X networks that use tunnelling EAP methods such as PEAP or EAP-TLS, user credentials are split into an outer identity and an inner identity. The outer identity—exposed only in the first EAP exchange—carries a realm for RADIUS routing while keeping the username anonymous; the inner identity, conveyed inside the encrypted EAP tunnel, contains the real identifier and is used for

Some of these research results were obtained from the commissioned research (No. 23610) by National Institute of Information and Communications Technology (NICT), JAPAN.

authentication. Consequently, the Access Network Provider (ANP) and any intermediate RADIUS proxies learn neither the user's real ID nor other sensitive attributes, thereby preserving anonymity at the network edge.

Yet roaming, billing, and incident response require a way to reconcile anonymity with uniqueness. RFC 4372 addresses this by introducing the Chargeable User Identity (CUI), a session-specific pseudonym generated by the IdP and returned to the ANP [4]. The CUI hides the real ID from the ANP and the RADIUS path but remains unique enough that the IdP can later map it back to the user through its audit logs.

Under this architecture, location privacy is likewise structurally protected: the IdP, which knows the real identity, never receives location data, whereas the ANP, which knows the access-point location, never learns the real identity. Renewing the CUI each session—or on a timed schedule—further prevents long-term linkage of a user's movements, making the scheme a widely accepted model for accountable anonymity in Wi-Fi roaming environments.

B. Technical Issues for Location-Aware Services

While the design described above offers strong location-privacy guarantees, it also imposes a critical technical limitation: even with explicit user consent, the system cannot simultaneously identify the user and exploit the user's current location to deliver personalized, location-aware services. Because the IdP, by design, never learns location data, it cannot drive authenticated region-specific services on behalf of its users. Conversely, the ANP, which does possess reliable location evidence, lacks access to the user's real identity and therefore cannot determine which user is present at which place. This mutual blindness prevents any service provider from tailoring content or functionality to an identified user at a known location, despite the user's willingness to allow it.

Several work-arounds have been explored. One approach appends RADIUS attributes such as Called-Station-Id [5] or Location-Information [3] to the RADIUS exchange so that the user's location reaches the IdP. Doing so, however, delivers raw location data directly to the IdP, thereby requiring (i) explicit prior consent from each user and (ii) a new protocol or governance layer by which the ANP can record and convey that consent status. Even when the IdP is a trusted entity—e.g. the user's home university—centralizing off-campus location data in a single organization may be operationally or ethically undesirable.

A second option introduces an app-based location broker: the user installs a client application that, with consent, transmits GPS coordinates or Wi-Fi-scan fingerprints to an independent broker, which then links those data to a pseudonymous identifier and forwards them to service providers. Because the broker operates outside the IdP/ANP trust domain, identity and location remain technically separated. The scheme, nevertheless, relies on self-reported location from the terminal; thus it is inherently vulnerable to spoofing [6] [7] and, by extension, to fraud and illicit incentive harvesting, raising non-trivial security concerns.

A third technique—already deployed in eduroam [1] and similar federations—identifies users by post-hoc log correlation. The ANP, any intermediate RADIUS proxies and the IdP each retain their own authentication logs; when an incident occurs, the relevant parties cross-match these records to pinpoint which user was on the network at a given time. This strategy delivers accountable anonymity: identity remains hidden during normal operation, yet can be uncovered when warranted. It is not, however, suited to use-cases that demand real-time, location-aware responses, because the necessary correlation is performed only on demand after the fact.

Thus, there is an inherent trade-off between the design principle of structurally protecting location privacy and the functional requirement of providing location-aware services to individuals. Building a new architecture that can provide accurate location proof while maintaining privacy, i.e., "accountable pseudonymous location proof," is an important technical challenge in modern roaming environments.

C. Related Work

This section surveys prior studies on Wi-Fi-based positioning and privacy protection.

Boutet et al. [8] proposed a high-accuracy Wi-Fi positioning scheme that preserves user privacy and introduces an explicit-consent mechanism for sharing location data, together with quantitative evaluation. Their work, however, did not address pseudonymity between the Identity Provider (IdP) and the Access Network Provider (ANP) or the particulars of RADIUS-based roaming authentication.

Yamaguchi et al. [9] addressed the operational and administrative challenges of deploying a nationwide roaming system across more than a thousand Japanese research and education institutions. To cut operating costs while safeguarding users' location privacy, they proposed a centrally aggregated, delegated-authentication system that relies on pseudonymous user identifiers.

Robert et al. [10] analyzed the legal implications of deploying Wi-Fi roaming and the security risks that arise while a mobile device establishes a roaming connection to the Internet. They compared direct access—in which a device reaches the Internet through the visited network—with tunnel access, where traffic is tunneled back to the home network, discussing security, legal duties and possible business models for each. Detailed privacy-protection mechanisms for end-users, however, remained outside their scope.

Yu et al. [11] focused on latency-sensitive applications such as VoIP and live streaming. They accelerated roaming by using 802.11v BSS Transition Management to collect signal and neighboring-AP data at the infrastructure side, perform on-the-spot localization and steer the client to the optimal AP. Their study concentrated on hand-over latency and link quality; it neither extended the technique to general location-aware services nor discusses location privacy.

Bernearos et al. [12] evaluated link-layer address randomization as a counter-measure to location tracking in Wi-Fi networks. They concluded that while MAC randomization mitigates the layer-2 privacy problem, additional upper-layer mechanisms are required to exploit its benefits fully and to minimize service disruption.

In sum, existing work addressed specific facets—precise positioning, legal frameworks, roaming performance, or MAC-level privacy—but did not integrate structural pseudonymity (e.g., CUIs) with consent-controlled, spoof-resistant location sharing across federated Wi-Fi roaming infrastructures, which is the focus of our study.

III. Location-Information Sharing Architecture

A. Overview of the Proposed Architecture

This section presents a location-information sharing architecture that adheres to a three-party separation model. The design simultaneously (i) structurally protects users' location privacy and (ii) allows precise location data to be used under explicit user consent. Building on the existing IEEE 802.1X / EAP / RADIUS Wi-Fi-roaming infrastructure, the scheme clearly separates the roles of the Identity Provider (IdP), the Access Network Provider (ANP), and a neutral Location Broker (LB) so as to realize accountable pseudonymous location proof.

At the core of the architecture is cooperation between the ANP and the Location Broker through the Chargeable User Identity (CUI) generated by the IdP during user authentication. The IdP derives a CUI from the user's real identifier and returns it to the ANP within the RADIUS authentication flow. The CUI uniquely identifies the session while preventing the ANP or any intermediate proxy from learning the user's real identity. Only when the user has given explicit consent does the Location Broker use the CUI as a key to query the ANP for the access-point location associated with that session. The broker can then safely bind the user's pseudonym to the contemporaneous location data and supply verified information to location-aware services.

A key feature of the design is that identity and location data travel through the network structurally separated, yet can be merged—under strict, consent driven conditions—by a single, trusted party. The IdP never learns location, and the ANP never learns the user's real identity; only the Location Broker is permitted to combine the two, and then only to the minimum extent authorized by the user. The broker works with a semi-permanent pseudonym rather than the real name; each session's short lived CUI is linked to this longer lived alias, preserving anonymity while retaining uniqueness.

Optionally, the broker may also collect supplemental on device location cues (e.g., GPS fixes or Wi Fi scans) via a client application. Correlating these user side readings with the RADIUS derived access point data can further strengthen the evidential value of the location proof.

Overall, the proposed architecture seeks to balance privacy, security, and service usability, providing a new framework that raises the trustworthiness of location aware services while preserving robust user control over personal data.

B. Entities and Their Roles

The proposed architecture is built on the IEEE 802.1X / EAP / RADIUS framework and aims to deliver location aware services while structurally protecting users' location privacy. Following a three party separation principle, it clearly delineates the responsibilities and data scopes of three independent entities—augmented here with the service layer—so that no single party can learn both identity and location.

1) Identity Provider (IdP)

The IdP is the RADIUS server that performs user authentication and is the only party that holds the user's real identity and attributes. On successful authentication the IdP returns a Chargeable User Identity (CUI) in the RADIUS Access Accept. The CUI is uniquely bound to the real ID inside the IdP but appears as a non identifying pseudonym to all other parties. The IdP may cryptographically protect the CUI or a longer-lived alias, but that detail is outside the scope of this section.

2) Access Network Provider (ANP)

The ANP operates the physical Wi Fi infrastructure and is therefore the only party that observes the user's connection point—that is, the location. It sends the RADIUS Access Request, receives the Access Accept containing the CUI, and stores metadata such as AP ID, connection time and MAC address, forming a location profile. When the Location Broker later queries the ANP with a given CUI, the ANP returns accurate location data for that session. Because the CUI is pseudonymous, the ANP can never link the location to the user's real identity.

3) Location Broker (LB)

The LB is a neutral, independently operated information intermediary. Only when explicit user consent has been recorded (details in Section 3.3) does the LB accept a CUI, query the corresponding ANP for location, and bind that location to a pseudonymous user identifier. Optionally, the LB can gather supplemental on device location cues (GPS fixes, Wi Fi scans) via a companion app and correlate them with the network derived position, thereby strengthening the resulting location proof.

4) Location-Aware Service Provider (LSP)

An LSP consumes the pseudonym linked location information supplied by the LB to deliver services such as contextual content, notifications or environmental control. It never receives the user's real identity; service logic relies solely on the pseudonym and location data. Typical examples include location based coupons or real time crowding alerts for public facilities. Because all consent management and data fusion are handled by the LB, the LSP holds only the minimum data required, enabling rich functionality without infringing user privacy.

5) End User

The end user is the central figure in the architecture—both the originator of the network connection and the data subject who controls whether location information may be shared. The user's device joins the Wi Fi network via IEEE 802.1X; authentication is performed by the IdP, and the device's inner identity remains protected inside the EAP tunnel, invisible to the ANP and the Location Broker. For location sharing the user grants—or later revokes—explicit consent to the LB through an application UI or browser dialogue. The LB enforces this consent status within its trust domain. Thus the user can choose what data are shared, with whom, and to what extent, retaining meaningful control under the regime of structural anonymity.

By cleanly separating the information held and the responsibilities borne by each entity, and by ensuring that real identity and location are never concentrated in the same party, the architecture safeguards location privacy while still allowing legitimate, consent based fusion of the two when required.

C. Protocol Design and Information Flow

This section details the protocol stack and message flow among the IdP, ANP and Location Broker (LB). The architecture adds only minimal extensions to the standard IEEE 802.1X / EAP / RADIUS exchange so that location proof elements are obtained as soon as the user joins the

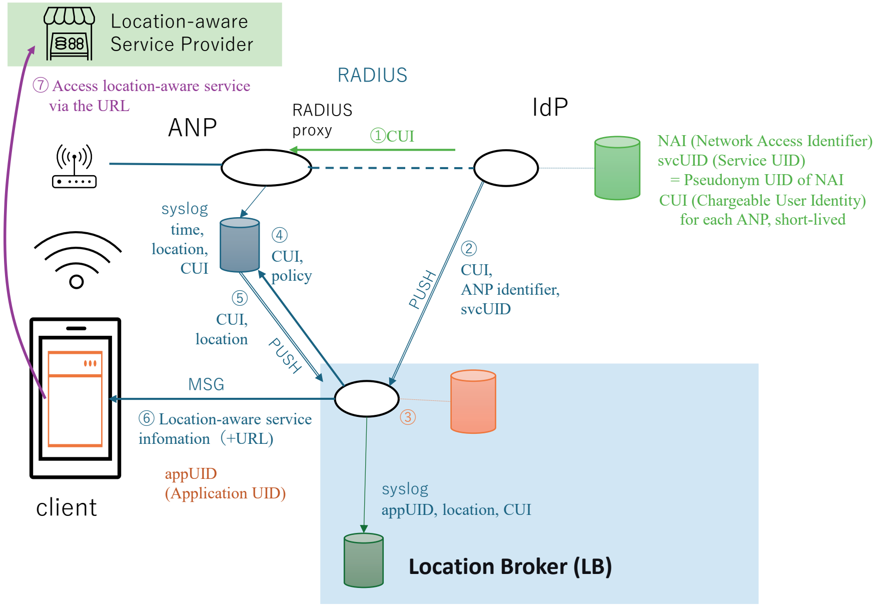

Figure 1. Protocol configuration and information flow in the proposed architecture.

network. The LB participates only when the user has given explicit consent and, even then, handles location queries solely through the pseudonymous CUI—never through the real identity. Figure 1 illustrates the representative flow:

1) Network Join and CUI Issuance

The client associates with an ANP access point and completes normal 802.1X authentication. The IdP issues a CUI for that session and returns it to the ANP in the RADIUS Access Accept.

2) CUI Push to the LB

Upon sending a new CUI, the IdP sends a push message to the LB—using any suitable push protocol—containing the CUI together with the user's pseudonym UID (svcUID as described later) and the ANP identifier.

3) Permission Policy Check

The LB consults the user's permission policy associated with the CUI to determine whether location sharing is allowed for the requesting ANP.

4) Policy Notification

If location sharing with that ANP is permitted, the LB returns the CUI and policy pair to the ANP.

5) Location Delivery

The ANP sends a push message containing the user's location to the LB in the granularity, scope and time resolution specified by the policy for each user movement.

6) Service Suggestion

Within the bounds of the user's policy, the LB matches the received location to the user's registered attributes and pushes a message to the client containing relevant location based service information and a URL.

7) User Action

The user reviews the offer and, if satisfied, follows the URL to interact with the location aware service provider.

D. Privacy Model and Security Evaluation

This section evaluates the privacy model provided by the proposed architecture and the resulting protection guarantees, with particular emphasis on how consent based location queries can be realized when the link identifier is a short lived pseudonym—the Chargeable User Identity (CUI).

Within the IEEE 802.1X / EAP / RADIUS framework the IdP issues a CUI after successful authentication. The CUI uniquely marks the session without revealing the real user identity and is conveyed to the ANP via the RADIUS path. The Location Broker (LB) later uses the CUI as a key when it queries the ANP for the location that corresponds to that session.

Because a CUI is by design anonymous, short lived and non reusable, the LB cannot intrinsically know whether a received CUI belongs to a user who has granted location sharing consent: the identifier changes every session, so any standing consent recorded earlier cannot be matched to the fresh CUI.

To resolve this issue, we introduce a semi-persistent UID (svcUID) on the LB that differs from the CUI. The svcUID is shared with the IdP binding pseudonymously to the actual user ID on the IdP. When a user pre authorizes location sharing, permission policy based on the user's consent is stored on the LB associated with the svcUID. During each authentication the IdP sends the new CUI to the ANP as usual and forwards the tuple {CUI, ANP identifier, svcUID} to the LB over a separate channel.

The benefit is that the CUI retains its anonymity and uniqueness toward the ANP, while consent management is delegated to a distinct channel; the CUI itself is never used as a consent token. Thus the CUI functions purely as a "location query handle," whereas the consent state is maintained inside the LB's trust domain—achieving a clean separation of responsibilities.

Crucially, any CUI based location query is honored only for sessions whose consent has been verified in advance. This requires the IdP to map real IDs to svcUIDs and the LB to exchange consent tokens with the user; both tasks can be implemented straightforwardly with existing federation technologies such as Shibboleth or OpenID Connect.

By dissociating the anonymous CUI from the semantic notion of user consent—and conveying the latter through an independent channel—the architecture realizes a secure and sustainable privacy model that reconciles location privacy with the provision of location aware services.

In practice, instead of notifying the LB of the CUI as in Step 2), the system can be modified so that the svcUID is encrypted and embedded into the CUI, as described in [13], and the ANP notifies the LB of the CUI in Step 3). This improvement allows the LB to understand the mapping between the CUI and the svcUID without direct communication between IdP and LB. It reduces the load on the IdP participating in this framework. In the proof-of-concept experiment described later, ECDH is used for key exchange for the encryption as explained in [14].

IV. Expected Use Cases and Applicability

In the previous section, we have shown that it is possible to achieve both privacy protection and consent-based location sharing by designing a separate management system for the pseudonymous identifier CUI and user consent. In this section, in order to clarify how this architecture can be applied to actual network environments and services, we assume several typical use cases and consider the applicability and advantages.

1) Integration with On-Campus Services

Universities utilizing Wi-Fi roaming infrastructure such as eduroam enable students and faculty to connect to the network via access points installed in multiple buildings and areas. By applying the proposed architecture, a location broker can identify the user's connection location using CUI, provided the user has explicitly consented, and integrate this information with campus services (e.g., library occupancy information, classroom availability, disaster evacuation guidance, etc.). Importantly, even if the university operates an IdP, location information is handled only through the broker, enabling consent-based service provision without the university itself knowing the user's location.

With the spread of online education and hybrid classes, there is growing interest in accurate attendance management and analysis of time spent in classrooms. If users consent to location sharing, the location broker can manage accurate attendance records based on Wi-Fi connection information and integrate them with educational support systems to visualize and optimize learning behavior. In this use case, the ability to flexibly set the scope of consent (e.g., limiting consent to entering a classroom on the day a registered class is held) is a key strength of the proposed architecture.

2) Incentive Distribution in Regional Tourism Apps

The proposed architecture is also effective for tourism apps that utilize regional collaboration Wi-Fi (e.g., OpenRoaming) at tourist destinations to provide coupons and information based on visitors' locations (Figure 2). When visitors agree to share their location in the tourism app, the location broker identifies their current location through CUI and enables location-aware content distribution by collaborating with affiliated stores and local government services. Tourists' real IDs are not disclosed within the app, and services are completed using pseudonymous identifiers, enabling a privacy-conscious structure that contributes to regional revitalization.

In this use case, for example, the LB can match user-registered attributes and push a URL for a discount coupon to visitors from other prefectures only when they enter a partnered store.

3) Collaboration with Public Agencies in Emergencies

In emergencies such as disasters, it is essential that location information be shared quickly and securely for evacuation guidance and safety confirmation. In the proposed architecture, the location broker can obtain the connection location through the CUI and provide it to public agencies or designated agencies only when the user has previously agreed to share information in emergencies.

For example, it is conceivable to send push-type surveys to disaster victims to inquire about necessary support, or to provide attributes such as the residential areas, age groups, and genders of disaster victims at each evacuation center to disaster-affected local governments or the disaster victims' residential areas to assist in planning secondary evacuations (Figure 3).

In such cases, real IDs remain under the management of the IdP and are not disclosed, thereby achieving both privacy protection in normal times and emergency response capabilities in times of crisis.

V. Concluding Remarks

This paper has tackled the long-standing tension between user privacy and location-aware functionality in federated Wi-Fi roaming. Building on the insight that the standard IEEE 802.1X / EAP / RADIUS stack already furnishes a trustworthy location proof—the access point itself, we have introduced a three-party architecture that keeps identity with the IdP and location with the ANP, employs the session-specific Chargeable User Identity (CUI) as a pseudonymous handle, and entrusts a neutral Location Broker to fuse CUI with location only under explicit user consent, thereby realizing an accountable pseudonymous location proof. We have analyzed its security and privacy properties, demonstrated resistance to location spoofing, and mapped the design to several practical scenarios—campus services, tourism incentives, and disaster-shelter support.

The architecture requires only minimal changes to the existing authentication flow: the IdP generates a CUI and pushes it to the Broker, and the Broker manages a separate consent channel. No modification of client devices or the 802.11 MAC layer is necessary. A proof-of-concept FreeRADIUS implementation is under internal test and shows negligible overhead in round-trip time.

Our model presumes a functioning trust fabric among IdPs, ANPs, and the Broker. Consent management introduces extra signaling and a UI burden on the user. Policy coordination across thousands of roaming domains remains challenging, and we have yet to quantify performance at continental scale. Finally, while spoof-resistant, the design does not address physical layer attacks such as rogue AP impersonation.

Next steps include: (i) an inter-regional pilot within OpenRoaming, (ii) integration of fine-grained consent revocation and real-time audit logs, (iii) performance benchmarking on an OpenRoaming backbone, and (iv) economic analysis of incentive schemes for ANPs and Location-aware Service Providers. We will soon start a proof-of-concept experiment in real-world environments across multiple regions, including commercial facilities in Sapporo and accommodation facilities in Kyoto, to verify whether data sharing under privacy constraints can effectively address regional challenges such as tourism promotion and emergency response by local governments [15].

Acknowledgment

We extend our deepest gratitude to Mr. Fukuie and Ms. Fushimi of the IKEUCHI Group for their discussions in preparation for the proof-of-concept experiment.

References

[1] K. Wierenga, S. Winter , T. Wolniewicz, “The eduroam Architecture for Network Roaming,” RFC 7593, Sept. 2015. [online]. Available: https://datatracker.ietf.org/doc/html/rfc7593.

[2] H. Goto, “Inter-federation Roaming Architecture for Large-scale Wireless LAN Roaming Systems,” Journal of Information Processing, pp. 103-112, 2021.

[3] H. Tschofenig (Ed.), “Carrying Location Objects in RADIUS and Diameter,” RFC 5580, Aug. 2029. [online]. Available: https://datatracker.ietf.org/doc/html/rfc5580.

[4] F. Adrangi, A. Lior, J. Korhonen, J. Loughney, “Chargeable User Identity,” RFC 4372, Jan. 2006. [online]. Available: https://datatracker.ietf.org/doc/html/rfc4372.

[5] C. Rigney, S. Willens, A. Rubens, W. Simpson, “Remote Authentication Dial In User Service (RADIUS),” RFC 2865, June 2000. [online]. Available: https://datatracker.ietf.org/doc/html/rfc2865.

[6] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, G. Lachapelle, “GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques,” International Jounal of Navigation and Observation, 2012.

[7] C. Hu, Y. Liu, Z. Lu, S. Zhao, X. Han , J. Xiong, “Smartphone Location Spoofing Attack in Wireless Networks,” In: SecureComm 2021, Canterbury, Great Britain (online), 2021.

[8] A. Boutet, M. Cunche, “Privacy protection for Wi-Fi location positioning systems,” Journal of Information Security and Applications, Vol. 58, 2021.

[9] I. Yamaguchi, T. Suzuki, H. Goto, H. Sone, “Centralized Authentication System for Location Privacy Protection and Low Operational Cost of Large Scale WLAN Roaming,” In: 10th IEEE/IPSJ International Symposium on Applications and the Internet, Seoul, Korea (South), 2010.

[10] R. Robert, M. Manilis, F. De Villengragne, D. Leroy, J. Jost, F. Koeune, C. Ker, J.-M. Dinant, Y. Roullet, O. Bonaventure, J.-J. Quisquater, “WiFi Roaming: Legal Implications and Security Constraints,” International Journal of Law and Information Technology, Vol. 16, No. 3, pp. 205-241, 2008.

[11] H. C. Yu, K. Alhazmi , R. R. Rao, “Wi-Fi Roaming as a Location-based Service,” In: IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020.

[12] C. J. Bernardos, J. C. Zúñiga, P. O'Hanlon, “Wi-Fi internet connectivity and privacy: Hiding your tracks on the wireless Internet,” In: IEEE Conference on Standards for Communications and Networking (CSCN), Tokyo, Japan, 2015.

[13] Y. Okabe, M. Nakamura and H. Goto, “Dynamic VLAN Assignment for Local Users Under External IdP Management in RADIUS-Based Wi-Fi Roaming,” In: 2024 International Conference on Information Networking (ICOIN), Ho Chi Minh City, Vietnam, 2024.

[14] H. Goto, “Offline Attribute Sharing Methods for Authentication Traffic Reduction and Functionality Enhancement of Wireless LAN Roaming Systems,” 2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC), Toronto, ON, Canada, 2025.

[15] Y. Okabe, H. Goto, E. Sakane,T. Hirose, “Privacy-Aware Inter-Regional Data Sharing of Local User Information in OpenRoaming, In: 2025 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 2025.

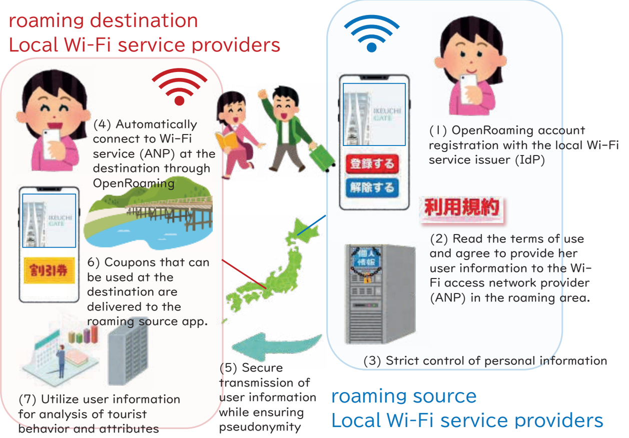
roaming destination
Local Wi-Fi service providers
(4) Automatically connect to Wi-Fi service (ANP) at the destination through OpenRoaming
IKEUCHI GATE
割引券
6) Coupons that can be used at the destination are delivered to the roaming source app.
(7) Utilize user information for analysis of tourist behavior and attributes
(5) Secure transmission of user information while ensuring pseudonymity
IKEUCHI GATE
登録する
解除する
(1) OpenRoaming account registration with the local Wi-Fi service issuer (IdP)
利用規約
(2) Read the terms of use and agree to provide her user information to the Wi-Fi access network provider (ANP) in the roaming area.
個人情報
(3) Strict control of personal information
roaming source
Local Wi-Fi service providers

Figure 2. Scenario for regional tourism apps.

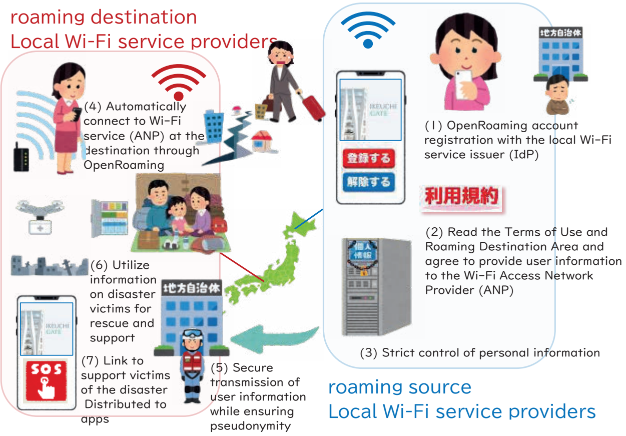
roaming destination
Local Wi-Fi service providers
(4) Automatically connect to Wi-Fi service (ANP) at the destination through OpenRoaming
(6) Utilize information on disaster victims for rescue and support
地方自治体
IKEUCHI GATE
SOS
(7) Link to support victims of the disaster Distributed to apps
(5) Secure transmission of user information while ensuring pseudonymity
地方自治体
IKEUCHI GATE
登録する
解除する
(1) OpenRoaming account registration with the local Wi-Fi service issuer (IdP)
利用規約
(2) Read the Terms of Use and Roaming Destination Area and agree to provide user information to the Wi-Fi Access Network Provider (ANP)
個人情報
(3) Strict control of personal information
roaming source
Local Wi-Fi service providers

Figure 3. Scenario for disaster evacuation shelters.