Dynamic VLAN Assignment for Local Users Under External IdP Management in RADIUS-Based Wi-Fi Roaming

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

Motonori Nakamura
Academic Center for Computing and Media Studies
Kyoto University
Kyoto, Japan
nakamura.motonori.2c@kyoto-u.ac.jp

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

***Abstract*—In a RADIUS-based Wi-Fi roaming architecture such as eduroam, a guest user is authenticated by his home Identity Provider (IdP) based on the Radius hierarchy, while a local user of the Service Provider (SP), the organization which serves the access points, is authenticated by an internal RADIUS server. Using this, it's possible to configure settings such that local users are connected to dedicated local VLANs for them through the dynamic authenticated VLAN technique. However, when ID management is outsourced to an IdP operated by an external organization, there is no mechanism to securely identify local users from guest users, making it impossible to give them local access. In this paper, we propose a mechanism for RADIUS-based Wi-Fi roaming architecture that allows local users to access local network resources while preserving the privacy of guest users. An IdP entrusted with identity management sends the authenticated user's identifier encrypted with the shared key of the home organization of the user as CUI (Chargeable User Identity) attribute, so that the RADIUS proxy of the home organization can securely identify local users, while the identifier appears as if it were a temporary random value to RADIUS proxies that do not have the encryption key.**

Keywords—RADIUS, Wi-Fi roaming, dynamic authenticated VLAN, eduroam, OpenRoaming, Chargeable User Identity (CUI), EAP, outer identity

I. INTRODUCTION

Public Wi-Fi has become an indispensable infrastructure in today's world, playing a pivotal role in ubiquitous connectivity. With prevailing challenges in security and convenience in conventional Wi-Fi spots, there is an increasing demand for a global Wi-Fi roaming architecture that enables people everywhere to connect securely and effortlessly to public Wi-Fi networks. Following the success of eduroam [1], there is a growing anticipation surrounding OpenRoaming [2,3]. As an initiative aimed at creating a seamless handover experience between Wi-Fi networks and cellular, OpenRoaming is poised to revolutionize public Wi-Fi access.

Eduroam provides Wi-Fi network access to members outside the organization as guests, but if guest users were allowed to connect directly to the organization's internal network, they would be allowed to use services that restrict access by IP address, such as electronic journals, to people outside the university. Therefore, it is customary to assign a dedicated VLAN for guests so that they can connect to the outside network using a different IP address. At the same time, for users belonging to the organization, they can be connected to the internal network using dynamic VLAN assignment upon successful authentication [4]. Since authentication is performed by the organization's IdP via the organization's internal RADIUS server for a local user, the IdP can know who the user is and which internal affiliation he belongs and can communicate the corresponding dynamic VLAN assignment to the access point via RADIUS. However, this mechanism does not work when ID management is outsourced to an IdP operated by an external organization and the realm of the outsourced IdP is used for the ID, because there is no mechanism to securely identify a local user from a user outside the organization. Although the IdP of the consignee can distinguish a local user of the consignor organization from a user outside the organization, there is no mechanism to securely communicate this fact from the IdP to the network access provider (NAP) via RADIUS.

In this paper we propose a mechanism for RADIUS-based Wi-Fi roaming such as eduroam and OpenRoaming to securely allow local users to access local network resources while protecting user privacy, even when identity management is outsourced to an IdP outside the organization. By sending an identifier that can locally identify an authenticated user as a CUI (chargeable user identity) attribute in RADIUS encrypted with a pre-shared key from an external trusted authentication server to a local RADIUS proxy, the information that can identify the user is conveyed securely to the RADIUS proxy at NAP. The external authentication server that is entrusted with authentication sends an identifier that can locally identify the authenticated user to the home RADIUS proxy as a CUI, encrypted using a pre-shared key, to the RADIUS. The value of the CUI is visible to other RADIUS servers that do not have the pre-shared key as a temporary, random value, similar to a CUI based on a conventional hash value, thus protecting the user's privacy. For the implementation study, we adopt AES128GCM defined in RFC8188 as the encryption scheme.

The rest of this paper is organized as follows. In Section II basic concepts on RADIUS-based Wi-Fi roaming are described. In Section III, we first introduce eduroam and OpenRoaming global Wi-Fi roaming architectures, then argue on issues in dynamic VLAN assignment for local users under external IdP management, and present our solution using a CUI. Section IV describes security considerations, and Section V provides a brief summary.

Some of these research results were obtained from the commissioned research JPJ012368C04401 by National Institute of Information and Communications Technology (NICT), JAPAN.

II. Basic Concepts

A. RADIUS and EAP

RADIUS (Remote Authentication Dial-In User Service) [5] is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. RADIUS servers manage a database of user profiles that all remote access servers use for security purposes, allowing for scalability and centralized management of user credentials.

A RADIUS proxy, on the other hand, acts as an intermediary between RADIUS clients and servers. It forwards authentication and accounting requests to the appropriate RADIUS server, often across different domains. The proxy does not make final authentication decisions but rather relays information between the client and one or more RADIUS servers which perform the actual verification of the user's credentials. This is particularly useful in scenarios where users are roaming between different networks or organizations but need a seamless authentication experience.

The Extensible Authentication Protocol (EAP) [6] is an authentication framework which supports multiple authentication methods. RADIUS servers that utilize EAP are capable of facilitating a broad range of authentication mechanisms such as passwords, certificates, etc. In RADIUS implementations, EAP is used to relay authentication data between a supplicant (user device) and an authentication server (IdP), typically through intermediaries such as an Wi-Fi access point and some RADIUS proxies, which is relevant in wireless network access.

EAP messages are encapsulated within RADIUS packets and forwarded to the RADIUS server for interpretation and authentication using the appropriate method. User devices generate EAP messages and encapsulate them within RADIUS packets to send to the authentication server. The server processes these messages, authenticates the user, and returns the result encapsulated in a RADIUS packet back to the device. Thus, RADIUS and EAP operate in conjunction, especially in environments like wireless networks, to provide secure and efficient user authentication.

In RADIUS authentication, particularly when using EAP-based methods, two different identities are employed: the *outer identity* and the *inner identity*, which are crucial in tunnel-based authentication methods like EAP-TTLS [7] or EAP-PEAP. Outer Identity is the identity used initially to establish the tunnel. It is often anonymized to conceal the user's actual username or device information (e.g., `anonymous@example.com`). The purpose is to protect the user's real identity on public networks or from other receiving devices. After the tunnel is established, the inner identity is used within the actual authentication process. It includes the user's real username or other authentic credentials, hidden from external observers or attackers within the tunnel. The use of these dual identities enables the secure transfer of authentication information while concealing the user's true details.

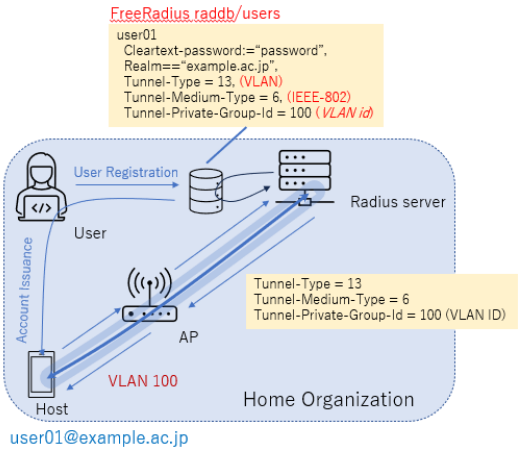

Fig. 1 Dynamic authenticated VLAN assignment based on RADIUS.

B. Chargeable User Identity (CUI)

Chargeable User Identity (CUI) is an extension to the RADIUS protocol, designed to anonymize or maintain consistency in user identity information for billing purposes.

Key purposes and features of CUI include:

- Anonymizing Identity: In a standard RADIUS authentication process, the user's real identity (e.g., username) may be included in the request/response. CUI replaces this information with a unique identifier to protect user privacy.
- Consistency Across Multiple RADIUS Servers: CUI allows for consistent identification of users across different RADIUS servers within a network or across different providers for billing information.
- Streamlining RADIUS Requests/Responses: Using CUI reduces the amount of real user information in requests and responses, making RADIUS communication more efficient.

CUI is specifically implemented as the Chargeable-User-Identity attribute in RADIUS messages. In an initial authentication request, the CUI remains unset, but the RADIUS server includes the CUI attribute in the authentication response, which can then be used for subsequent transactions. This functionality is particularly effective in large-scale networks or scenarios involving roaming between multiple service providers.

As an example of the CUI generation algorithm, the following is shown in the FreeRadius source code [9]:

```
Chargeable-User-Identity=
  "%{sha1:${policy.cui_hash_key}%{tolower:%{User
  -Name}%{%{Operator-Name}:-}}}"
```

Here `cui_hash_key` should be chosen as a random string so as to protect CUI values against dictionary attacks. CUI is generated from both User-Name and Operator-Name and hance user anonymity across operators is maintained.

C. Dynamic authenticated VLAN

Dynamic authenticated VLAN refers to dynamically assigning a Virtual Local Area Network (VLAN) after successful authentication [10]. During authentication, a client provides credentials to access the network. A RADIUS server verifies these credentials and returns a success or failure response to the network switch or access point. If authentication succeeds, the server includes specific VLAN information in its response, indicating the network segment the user should access. The switch or access point then

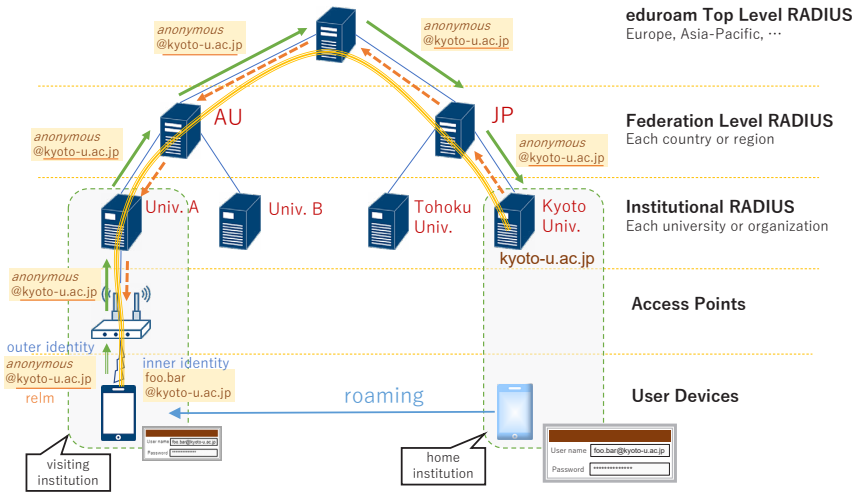

Fig. 2 eduroam RADIUS hierarchy.

dynamically assigns the client's traffic to the appropriate VLAN based on this information.

In assigning dynamic authenticated VLAN, several RADIUS attributes are used to direct the dynamic assignment of VLANs and other tunnel configurations. The following are descriptions of particularly important attributes:

- Tunnel-Type: Specifies the type of tunnel; for VLAN assignments, the value typically used is "VLAN" (value 13).
- Tunnel-Medium-Type: Specifies the tunnel's media (physical) type. Values include "802" (value 6) for IEEE 802 (Ethernet) and "IP" (value 1) for IP. For VLAN settings, "802" is commonly used.
- Tunnel-Private-Group-ID: Specifies the VLAN ID; for example, the value "100" would assign a user or device to VLAN 100.

These attributes are returned in the response from a RADIUS server to an access request, and the access server (like a switch or access point) interprets these attributes to dynamically assign users or devices to the specified VLAN (Fig. 1). This mechanism allows organizations to dynamically control access to network resources based on criteria such as user or device type, role, and group membership using a centralized authentication server.

III. Dynamic Authenticated VLAN Assignment for Local Users

A. eduroam

eduroam [1] is a wireless LAN roaming service developed for the international research and education community. Students, researchers, and staff from participating organizations can connect to Wi-Fi at any participating campus using their home organization's account credentials. eduroam has been rolled out in many countries and regions around the world, providing secure wireless LAN access among participating research and education institutions. This structure facilitates wireless LAN connectivity for researchers and students when visiting different campuses and institutions.

The core technology behind eduroam is RADIUS-based authentication [11]. When a visiting user tries to connect to an eduroam network on a campus other than his own, the authentication request is first sent to the local RADIUS proxy of the campus. The request is forwarded through a hierarchical network of RADIUS proxies to the user's home organization's server, where authentication is performed, and the result is sent back to the access point to which the roaming user is connecting. eduroam employs WPA2 Enterprise authentication and uses EAP methods for secure communication of authentication information with RADIUS servers, minimizing the risk of credential leakage.

Fig. 2 illustrates how eduroam authentication works through the RADIUS hierarchy. In this example, a user from Kyoto University (`foo.bar@kyoto-u.ac.jp`) visits Univ. A in Australia (AU). The user device first associates with the Wi-Fi access point, and then sends `anonymous@kyoto-u.ac.jp` as the outer identity and the EAP method through the IEEE802.1x authentication procedure. The authentication request is converted to the RADIUS protocol at the access point, and based on the relm part of the outer identity, `@kyoto-u.ac.jp`, a path of RADIUS proxies is established as the Univ. A's RADIUS server, the AU proxy, the Asia-Pacific proxy, the JP proxy, to reach the Kyoto-U RADIUS server. Here, a secure tunnel based on EAP is established between the user device and the Kyoto University's authentication server, and the authentication result is returned to the access point by RADIUS through the reverse direction of the path. Here, the AP of the visiting organization and the relaying RADIUS proxies can see the outer identity of the user, so they know that a user from Kyoto University is using this network access. However, since the inner identity is not visible to them, it is not possible to identify which user of Kyoto University is using it, thereby preserving user anonymity.

To balance the need for anonymity with the practicality of incident handling, eduroam employs a Chargeable User Identity (CUI) attribute accompanied by the Operator-Name attribute. These attributes refine the accounting process by reducing anonymity but preserving pseudonymity. This approach also enables NAPs to implement policies like restricting the number of devices that a user can have connected, for example.

B. *OpenRoaming*

OpenRoaming [3] is a wireless network solution that allows devices to automatically connect to Wi-Fi networks seamlessly and securely. It's designed to bridge the gap between Wi-Fi and cellular networks, providing users with a better roaming experience. OpenRoaming is managed by the Wireless Broadband Alliance (WBA), a consortium that works to improve the Wi-Fi experience and develop seamless wireless network services globally. The WBA took over the management and development of OpenRoaming from Cisco, which initially developed the concept. The WBA oversees the OpenRoaming framework, working with its members, which include technology providers, mobile operators, and network providers, to expand the OpenRoaming service and its adoption. The benefit of OpenRoaming is that it enables a more seamless and user-friendly Wi-Fi experience, especially for those moving across different locations, without the friction usually associated with connecting to new Wi-Fi networks. It also benefits network providers by allowing them to offer value-added services and maintain customer satisfaction with reliable connectivity.

Just like eduroam, OpenRoaming achieves a federation of Wi-Fi networks through a RADIUS hierarchy. While eduroam provides seamless connectivity through the common use of a single ESSID `eduroam`, OpenRoaming offers a more sophisticated automatic connection that does not rely on ESSIDs, by adopting the Wi-Fi Certified Passpoint technology. GÉANT, which oversees the global eduroam federation, is a founding member of WBA OpenRoaming and is studying the possibility of integrating next-generation eduroam and OpenRoaming [12].

OpenRoaming supports SIM-based authentication methods, such as EAP-SIM, EAP-AKA, and EAP-AKA' [13] which are commonly used by mobile carriers. Those authentication methods use SIM (Subscriber Identity Module) credentials for authentication, which are securely stored on the user's mobile device. Upon attempting to connect to an OpenRoaming-enabled Wi-Fi network, a device can select from various authentication methods, including e.g. EAP-AKA if available, using its SIM card for the process. The device's authentication request is sent to the Wi-Fi, then is forwarded to the carrier's RADIUS server, which verifies the SIM credentials with the carrier's authentication server. Once validated, the RADIUS server confirms the device's authentication and informs back the Wi-Fi network that the device has been authenticated.

OpenRoaming incorporates a mechanism known as "WBA IMSI Privacy Protection" to safeguard user privacy [14]. This mechanism ensures that the International Mobile Subscriber Identity (IMSI) is not exposed to the Wi-Fi access point nor the RADIUS proxies which forward the request during the authentication process. The specifics can be found in Fig. 3, which depicts the Inner Identity structured as <IMSI>`@wlan.mnc`<MNC>`.mcc`<MCC>`.3gppnetwork.org`. Here, the MCC (Mobile Country Code) is generally a three-digit number that identifies a particular country or region, and the MNC (Mobile Network Code) is a two or three-digit number that, when used alongside the MCC, pinpoints a specific mobile operator within that country. The Outer Identity is formatted as <EAP-Method>`anonymous@wlan.mnc`<MNC>`.mcc`<MCC>`.3gppnetwork.org`. While the MCC and MNC are visible to the access point and the traversing RADIUS proxy, the IMSI remains concealed.

The WBA OpenRoaming stipulates that the CUI is mandatory in Access-Accept response when the user identity is encrypted, such as in SIM-based authentication.

C. *An issue in dynamic VLAN assignment for local users*

In eduroam, a network access provider facilitates Wi-Fi access for visiting users, ensuring they do not penetrate the organization's restricted internal network services, such as electronic journals, by allocating a distinct VLAN for guest connections to utilize alternate IP addresses. Additionally, it is possible to configure the network so that its own eduroam users gain access to the internal network via dynamic VLAN assignments post-authentication. For local users, authentication through the organization's IdP via its RADIUS server enables identification of the user's internal affiliation, prompting the assignment of an appropriate dynamic VLAN to the access point (Fig. 4).

However, this assignment process is compromised when ID management is delegated to an external IdP using a different realm, as the secure recognition of local versus cannot be conveyed to the network access provider through

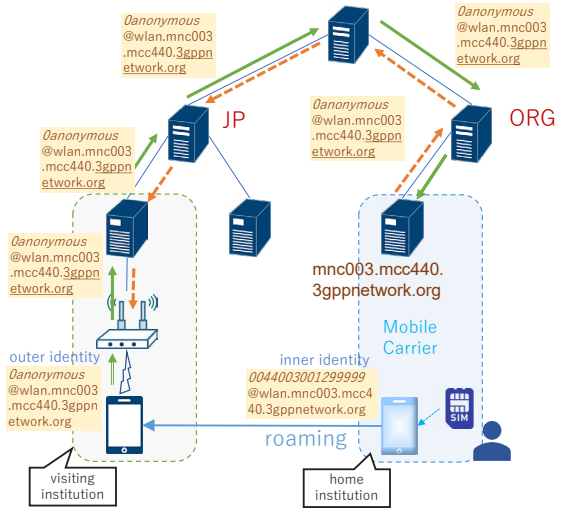

Fig. 3 WBA IMSI Privacy Protection for Wi-Fi.

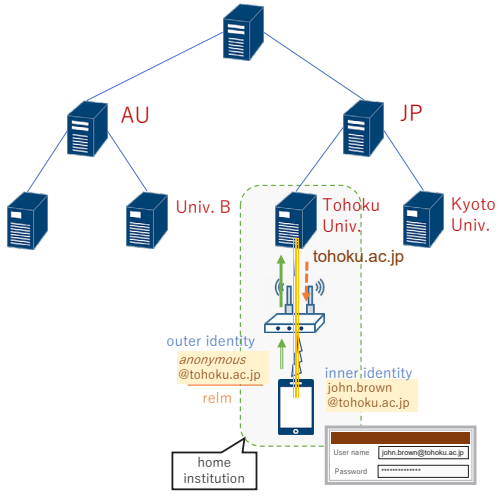

Fig. 4 Authentication and dynamic VLAN assignment for a local user.

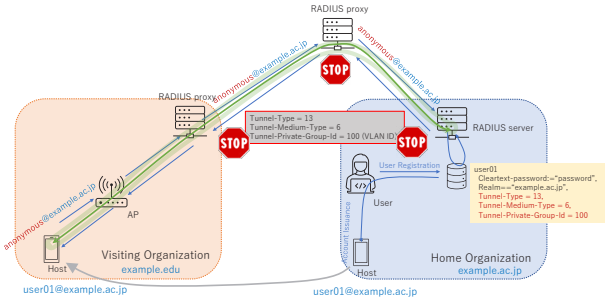

Fig. 6 Dynamic authenticated VLAN doesn't work when roaming.

the current RADIUS framework. While the contracted IdP can discern local users of the organization from visiting guests, it lacks a secure method to relay the VLAN assignment associated with this distinction to the network access provider. Details are shown in Fig. 6. In general, even if dynamic VLAN assignment is defined for each user at the home organization, this information will not be sent out to the outside of the institution nor will not be relayed by the intermediate RADIUS proxies. Even if the visiting organization receives an attribute for dynamic VLAN assignment, such as Tunnel-Private-Group-Id, from outside the institution, it should be discarded. Since these attributes are relayed through unsecured communication paths in RADIUS, even if there is an agreement between the home and visiting institutions, they cannot be used because the risk of tampering or forgery in the RADIUS relay paths cannot be ignored. This is reasonable behavior in the general case, but it also means that if authentication is done by an external IdP and the user is trying to connect to eduroam at his own institution, there is no way to give local access to the local user via dynamic VLAN assignment.

The eduroam JP Federated ID Service [15], an external IdP management based on the GakuNin Shibboleth federation provided by National Insutitute of Informatics (NII), avoids this problem by embedding the name of the organization and whether the user is a student or a faculty member in the realm part of the user ID, like `@kyoto-u.f.eduroam.jp` for a faculty member of Kyoto University (Fig. 5). However, the realm part is not necessarily trustable because it is exchanged unprotected as an outer identity in RADIUS, and it is undesirable from the viewpoint of privacy protection in that it may unnecessarily disclose information about the concerned user to unrelated organizations.

A similar situation can arise with OpenRoaming when using SIM-based authentication. Consider a company that has corporate contracts with a mobile carrier for employee mobile lines. At OpenRoaming-enabled Wi-Fi access points within

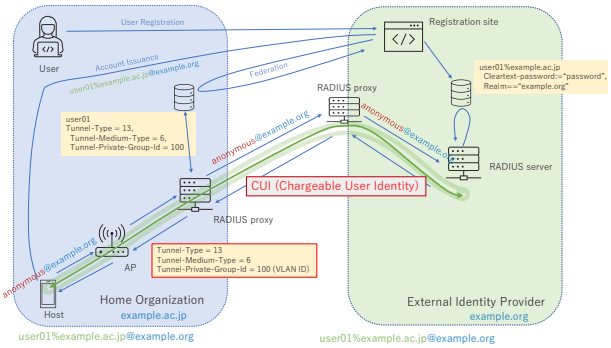

Fig. 7 Use of encrypted CUI for communicating user identity.

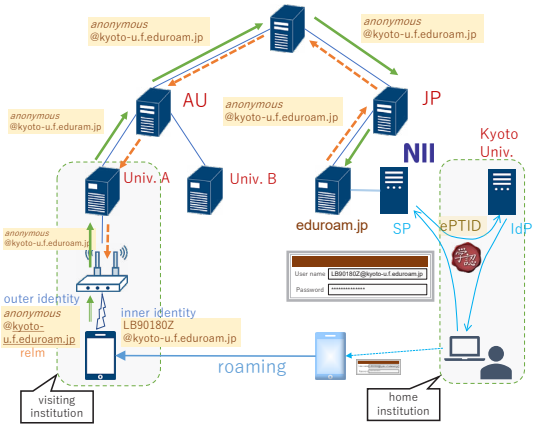

Fig. 5 eduroam JP Federated ID Service.

the company, they may want to grant dedicated access only to those lines recognized as belonging to employees. While the mobile carrier can verify that the contract is associated with a device belonging to a member of the company through SIM authentication, as discussed in Section III.B, OpenRoaming's SIM authentication only reveals the carrier's identity through the MCC and MNC in the outer identity's realm, lacking a secure method to convey the user's organizational affiliation.

D. Use of encrypted CUI

To address the aforementioned issue, we propose a secure transmission protocol for real user identities from the RADIUS server of an externally managed IdP to the RADIUS proxy of the user's home organization. This would be achieved by pre-establishing a shared secret key between the external IdP and the home organization. The real user identity would be encrypted using symmetric key cryptography and transmitted as a Chargeable User Identity (CUI).

As an example, consider the situation shown in Fig. 7. Here the domain of the user's home organization is `example.ac.jp`, and the domain of the external IdP is `example.org`. When a user registers his account with the external identity provider, he is guaranteed to have an identity at the home organization to which he belongs through authentication federation using SAML, and is issued an account with `user01%example.ac.jp@example.org` as the user ID for the external IdP. When this user accesses a Wi-Fi access point of the organization to which he belongs with this ID, the outer identity should be `anonyumous@example.org`, and hence the organization cannot identify the user as belonging to their organization without modification. Therefore, the Access-Accept response when the external IdP successfully authenticates the user is modified to include the user's real ID `user01%example.ac.jp` as CUI encrypted with the common key. The RADIUS proxy at the home organization that has the symmetric key can decrypt it, confirm the real ID, refer to the information on dynamic VLAN assigned to the user in the local database, and send it as attributes to the access point.

While the user's real ID is transmitted in an encrypted format in this example, it's only necessary to send an identifier that the home organization can use to recognize the specific user. For instance, when an account is registered at an external IdP via a Shibboleth/SAML federation, a pseudonymous identifier, such as an eduPersonTargetedID, can be utilized.

This approach preserves the user's anonymity relative to the external IdP.

E. Encryption by AES128GCM

In the proposed framework, the choice of encryption algorithm for the symmetric key cipher is flexible. However, considering that a Chargeable User Identity (CUI) is limited to a maximum of 253 bytes, an encryption mechanism that operates efficiently with short data sequences is preferable. Furthermore, given the expected high rate of CUI generation at the RADIUS server during authentication, a lightweight and rapid encryption algorithm is advantageous. To meet these criteria, AES-128-GCM, as specified in RFC 8188 "Encrypted Content-Encoding for HTTP," [16] is employed.

Data encoded in AEC128GCM has as a header a 16-byte salt, a 4-byte record size, an idlen that is the length of the keyid in 1 byte, a keyid in the idlen bytes, followed by a byte sequence of the length of the record size (TABLE I). Note that RFC2865 and RFC4372 assume CUI is a string which is any 8-bit octet sequence not terminated by the null character.

TABLE I. ENCRYPTION CONTENT-CODING HEADER

salt	rs	idlen	keyid
16	4	1	idlen

IV. SECURITY CONSIDERATIONS

As is stated in RFC4372, RADIUS entities (RADIUS proxies and clients) outside the home network must not modify the CUI or insert a CUI in an Access-Accept response, but there is no way to detect or prevent this. In contrast, a CUI encrypted with AES128GCM cannot be tampered with or forged by an attacker who does not have the corresponding shared key. If a CUI received by the network access provider does not conform to the AES128GCM format or the encryption key does not match, the CUI may be considered ordinary hash-based one. External IdPs can confirm the institution to which a user belongs through authentication, but they can only determine from which network access provider the user is accessing from the Operator-Name attribute. Therefore, even if the CUI is encrypted using a common key with the user's home organization, it might be received by another organization. In such cases, the user will treated as an ordinary visitor and no security violation will occur.

This paper does not show how the common key is shared between the home organization and the external IdP. If both parties participate in a Web federation as described in the example in Section III.D, a secure communication channel using public key cryptography can be ensured. A keyid must be chosen so that it does not conflict with the keyid of the key shared by the other party on each side. Therefore, it is desirable to make the idlen enough long so that there will be no difficulty in selecting the keyid without collision. Since the proposed scheme allows two parties to use multiple keys at the same time, they can operate in parallel for a certain period of time when switching keys. For forward security considerations, it is desirable to switch keys periodically.

The proposed method assumes that external Identity Providers (IdPs) are enough trustworthy, and it is vulnerable to malpractice by these external IdPs. If an external IdP were intentionally or mistakenly to authenticate a user from outside as a member of the organization and communicate the result via CUI, the user would improperly gain access to the organization's internal network VLAN. If such risks cannot be ignored, it is necessary to limit the internal resources that can be accessed via the dynamically assigned VLANs provided by this scheme.

V. CONCLUDING REMARKS

In this paper, we have addressed the challenge of providing local network access to local users through dynamic authenticated VLAN in RADIUS-based Wi-Fi roaming like eduroam, particularly when identity management is outsourced to an external IdP. To overcome this issue, we have suggested a secure method for transmitting an encrypted inner identity via the Chargeable User Identity (CUI) using a shared key cryptography.

We are currently working on a prototype implementation based on the proposed method using FreeRadius and the open source RFC8188 implementation. We hope to complete the prototype as soon as possible, release it to the public, and incorporate it into the eduroam JP federated ID service for practical use.

REFERENCES

[1] W. Klass, F. Licia, "Eduroam: past, present and future," Computational Methods in Science and Technology, vol. 11 (2), pp. 169-173, 2005.

[2] H. Goto, "Inter-federation roaming architecture for large-scale wireless LAN roaming systems," Journal of Information Processing, vol. 29, pp. 103-112, 2021.

[3] Wireless Broadband Alliance, "OpenRoaming," https://wballiance.com/openroaming/ (accessed: Nov. 6, 2023).

[4] Jisc, "FAQs for eduroam system administrators and implementation techs – Part 1," https://community.jisc.ac.uk/library/janet-services-documentation/faqs-eduroam-system-administrators-and-implementation-techs (accessed: Nov. 6, 2023).

[5] C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote authentication dial in user service (RADIUS)," RFC2865, June 2000.

[6] B. Aboba, P. Calhoun, "RADIUS (remote authentication dial in user service) support for extensible authentication protocol (EAP)," RFC3579, Sept. 2003.

[7] P. Funk, S. Blake-Wilson, "Extensible authentication protocol tunneled transport layer security authenticated protocol version 0 (EAP-TTLSv0)," RFC5281, Aug. 2008.

[8] F. Adrangi, A. Lior, J. Korhonen, J. Loughney, "Chargeable user ientity," RFC4372, Jan. 2006.

[9] FreeRADIUS project, https://github.com/FreeRADIUS/freeradius-server/blob/master/raddb/policy.d/cui (accessed: Nov. 6, 2023).

[10] P. Congdon, M. Sanchez, B. Aboba, "RADIUS attributes for virtual LAN and priority support," RFC4675, Sept. 2006.

[11] W. Wierenga, S. Winter, T. Wolniewicz, "The eduroam architecture for network roaming," RFC7593, Sept. 2015.

[12] K. Meyer, "OpenRoaming and eduroam – useful information for eduroam identity providers and service providers," https://www-stage.eduroam.org/openroaming-and-eduroam-useful-information-for-eduroam-identity-providers-and-service-providers/ (accessed: Nov. 6, 2023).

[13] J. Arkko, V. Lehtovirta, P. Eronen, "Improved extensible authentication protocol method for 3rd generation authentication and key agreements (EAP-AKA')," RFC5448, May 2009.

[14] Wi-Fi IMSI Privacy Protection Group, "IMSI privacy protection for Wi-Fi – technical specification, version 1.0," Wireless Broadband Alliance, Feb. 2021.

[15] NII ninsho, "User's guide (eduroam JP Federated ID Service)," https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=23855618 (accessed: Nov. 6, 2023).

[16] M. Thomson, "Encrypted content-encoding for HTTP," RFC8188, June 2017.