IEEE P802.11
Wireless LANs

|  |
| --- |
| ANQP Elements Augmentation Proposal |
| Date: 2021-07-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jerome Henry  | Cisco Systems |  |  | jerhenry@cisco.com |
| Stephen McCann | Huawei |  |  | Stephen.mccann@ieee.org |
| Bart Brinkman | Cisco Systems |  |  | bbrinkm@cisco.com |

Abstract

This submission proposes two new elements for ANQP that would be of use for WFA and federations use cases.

All the changes are related to Draft P802.11REVme D0.0.

|  |  |  |  |
| --- | --- | --- | --- |
| **CID** | **Comment** | **Proposed Change** | **Resolution**  |
| **93** | **Modern networks allow more than one types of credentials, but may not allow all types** | **Specify credential types that can be advertised as allowed, along with the allowed validation method and required lifetime for these credentials** | **Revise, define a new ANQP element that clarifies which credentials are accepted, along with the acceptation method.** |
| **94** | **Privacy is a primary determinator for network attachment choice. Without knowing if the local network requires a real identity or accepts anonymous IDs, users are forced to reveal more than they want or need** | **Define a privacy indicator element that clarifies if the network allows for anonymous connections** | **Revise, define a Privacy indicator element for ANQP** |

**Discussion:**

* In large federations (where multiple venues may allow for multiple sources of identities), the multi-to-multi relationship makes it difficult for the STA profile to understand the required identity and credential expectations of the venue, and how these map to the identity profile that the STA is configured to use.
* This ambiguity can cause unnecessary overhead or may cause the STA to send discovery messages that may not be required by the infrastructure (and that can in turn, affect the user privacy or result in a lower user experience).
* This submission proposes additional ANQP elements that can assist a STA in clarifying the required identity and credential expectations of the infrastructure.
* In a multi-to-multi environment (e.g., multiple venue members of a federation), each venue may advertise a RCOI (Roaming Consortium) that allow STAs to provide multiple identities, each with different credential type requirements (e.g., simple email, proof of residence, identity validation or other). Each venue may also accept multiple types of credentials. However, the venue may also be constrained in the type of credentials it can accept (e.g., ‘only accept credentials where the user identity can be verified’) – this is a limitation in WBA and WFA scenarios
* It is useful to define the credential types that the venue can accept, as this may be a subset of the credentials accepted by all of the RCOI members within a federation (e.g., type of credentials accepted, with type of verification accepted, credential lifetime)
* The venue may also mandate that the user connects with a verifiable outer identity. In other cases, the venue requirements are satisfied with an anonymous outer identity, provided that an authentication source validates the user credentials. It may be useful to specify if the venue requires a ‘real’ outer identity or not, potentially removing the need for clients to expose their user identity where it is not needed.

***Proposed resolution:***

Revised.

***To editors: insert after 9.4.5.29***

Credential Types ANQP-Element

The Credential Types ANQP-element provides a STA with the information about the types of credentials accepted via that AP. One or more types of credentials are listed in the Credential Types subfield. The format of the Credentials Types ANQP-element is show in figure XX.

****

Figure XX - Credentials Types ANQP-element format

The Info ID and Length fields are defined in 9.4.5.1 (General).

The Credential Types subfield includes for each type of accepted credential, the credential type, the accepted validation methods, the minimum lifetime required for the credentials, and a privacy indicator. The format of the Credential Types subfield is shown in figure XX.

****

Figure XX - Credential Types subfield format

The credential category subfield includes a category of credentials accepted by an AP. The list uses category groups and category types from Table 9-66.

The validation method subfield lists the type of credential validation that must occur for the credentials to be deemed valid.

|  |  |  |
| --- | --- | --- |
| **Validation method** | **Value** | **Notes** |
| No verification | 0 | Credentials do not need to be verified |
| Any method allowed | 1 | Any method, from 1 to 5, is accepted |
| Email verification | 2 |  |
| SMS verification | 3 |  |
| Government ID | 4 | e.g., account obtained by showing a Government ID |
| Government issued credentials | 5 | e.g., a certificate emitted by a Government |
| Reserved | 6-7 |  |

The weakest supported method is indicated (e.g., a validation method of 3 indicates that methods 3, 4 and 5 are accepted).

The Lifetime subfield indicates the minimum age of the credentials to be acceptable, in units of year quarters (e.g., a value of 8 represents that the matching credentials are accepted if the account is 8 quarters or more, or 2 years, old; a value of 0 indicates that the matching credentials are accepted if they are 0 quarters or more).

When set, the Privacy indicator indicates that this network requires the user to expose a real contactable identity to the network (usually for legal purposes). The default value is 0, indicating that this network will accept anonymous roaming.

***To editors: insert at the end of Table 9-66:***

|  |  |  |
| --- | --- | --- |
| **Credential Category** | **Venue group code** | **Venue type code** |
| **Misc entities** | **12** | **12** |
| **Service Provider** | **12** | **1** |
| **Cloud or Social Media Provider** | **12** | **2** |
| **Cable Industry** | **12** | **3** |
| **Government**  | **12** | **4** |
| **Reserved** | **12** | **5-255** |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Comment** | **Proposed Change** | **Resolution**  |
| **95** | **Users offered the choice between 2 networks may prefer to attach to the one that provides the best SLA, or for which they have an offload agreement with. However, such indication is not provided, limiting the quality of the experience for the user** | **Define a settlement indicator, and an SLA indicator, that clarifies if the network will accept all roaming, offer paid services or free services only, and if the network supports a form of SLA.** | **Revise, define a new ANQP element that clarifies the settlement and SLA values for the network** |

***To editors: insert after 9.4.5.29***

SLA ANQP-Element

The Service Level Agreement (SLA) ANQP-element provides STA with the information about the type of roaming supported by the local network, and the SLA offered by the AP for a given roaming type. The format of the SLA ANQP Element is shown in Figure XX.



Figure XX – SLA ANQP-element format

The Info ID and Length fields are defined in 9.4.5.1 (General).

The Venue SLA Policy subfield includes, for each type of roaming settlement, the SLA level provided by the venue, and optionally details on that SLA. The format of the SLA Policy subfield is shown in Figure XX.

****

Figure XX - SLA Policy subfield format

The First Settlement Indicator and the Second Settlement Indicator subfields indicate a type of roaming service accepted by the venue. The values of the First Settlement Indicator and of the Second Settlement Indicator is specified in Table 1. The First SLA Indicator subfield indicates the SLA that the network offers for the first settlement. The values of the First SLA Indicator and of the Second SLA Indicator is specified in Table 2. When the Second Settlement Indicator is set to 0, the Second SLA value is also set to 0 and unused.

The SLA Details field is an optional string formatted in UTF-8 that indicates the details of the SLA (e.g., minimum bandwidth, max jitter or delay, etc.) The content of this subfield is beyond the scope of this specification.

**Table 1: Settlement Indicator**

|  |  |
| --- | --- |
| **Settlement Indicator Value**  | **Settlement** |
| **0** | **All** |
| **1** | **Free services** |
| **2** | **Paid services** |
| **3** | **Reserved**  |

**Table 2: SLA indicator**

|  |  |
| --- | --- |
| **SLA Indicator Value**  | **SLA Level** |
| **0** | **No SLA** |
| **1** | **Bronze** |
| **2** | **Silver** |
| **3** | **Gold**  |

**Discussion:**

* In large federations (where multiple venues may allow for multiple sources of identities) using RCOI, the multi-to-multi relationship makes it difficult for the STA profile to understand which member of the RCOI is actually accepted in the venue. In some cases, the RCOI includes a large group of entities, some of which provide identity services and own access networks, and some of which also competing with each other. In that case, some venues may not accept credentials from competing entities. Therefore, in complement to the RCOI, it is useful to define a list of excluded Realms, i.e. realms which credentials are not accepted by the local venue.

***To editors: insert after 9.4.5.29***

Excluded NAI Realm ANQP-Element

The Excluded NAI Realm ANQP-element provides a list of network access identifier (NAI) realms corresponding to SSPs or other entities whose networks or services are not accessible via this AP, even if they are members of a Roaming Consortium advertised by this AP. The format of the Excluded NAI Realm ANQP-element is shown in figure XX.



Figure XX – Excluded NAI Realm ANQP-element format

The Info ID and Length fields are defined in 9.4.5.1 (General).

The Excluded NAI Realm count field specifies the number of NAI realms included in the Excluded NAI Realm ANQP-element.

The Excluded NAI Realm Tuples field contains zero or more variable length Excluded NAI Realm Tuple subfields.

The format of the Excluded NAI Realm Tuple subfield is shown in Figure XX (NAI Realm Tuple subfield format).

****

Figure XX – Excluded NAI Realm Tuple subfield format

The Excluded NAI Realm Data Field Length subfield is equal to 3 plus the length of the Excluded NAI Realm subfield.

The Excluded NAI Realm Encoding subfield uses the same format as the NAI Realm Encoding Type subfield defined in 9.4.5.10.

The Excluded NAI Realm Length is the length in octets of the Excluded NAI Realm subfield.

The Excluded NAI Realm subfield is one or more Excluded NAI Realms and uses the same format as the NAI Realm subfield defined in 9.4.5.10.