IEEE P802.11
Wireless LANs

|  |
| --- |
| ANQP Elements Augmentation Proposal |
| Date: 2021-08-13 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jerome Henry  | Cisco Systems |  |  | jerhenry@cisco.com |
| Stephen McCann | Huawei |  |  | Stephen.mccann@ieee.org |
| Mark Hamilton | Ruckus/CommScope | 350 W. Java DrSunnyvale, CA | +1 303 818 8472 | mark.hamilton2152@gmail.com  |
| Mark Rison | Samsung Cambridge Solution Centre | SJH, CB4 0DS, U.K. | +44 1223 434600 | at samsung (a global commercial entity) I'm the letter emme then dot rison |
| Bart Brinkman | Cisco Systems |  |  | bbrinckm@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***

Subclause: 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 Credential Types ANQP-element is shown in Figure XX.

 ****

Figure XX - Credential Types ANQP-element format

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

The Credential Types Count field indicates the number of Credential Types fields (i.e., *M* in Figure XX)

The Credential Types subfield includes a list of one or more Credential Types subfields, one for each type of accepted credential. The format of the Credential Types subfield is shown in figure XX.

****

Figure XX - Credential Types subfield format

The Category Group and Category Type subfields specify the credential issuer accepted by the AP. The Category Group and the Category Type subfields use values from Table 9-66. The Category Group and the Category Type values map to the Venue group code and the Venue list code in Table 9-66, respectively.

The Validation subfield is a bitmap that lists the type of credential validation that must occur for the credentials to be deemed valid.

|  |  |  |
| --- | --- | --- |
| **Validation method** | **Set Bit** | **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 Lifetime subfield indicates the minimum age required for the credentials to be acceptable, in units of year quarters.

The Privacy Indicator subfield is set to 1 if this network requires the user to expose a real contactable identity to the network (usually for legal purposes). It is set to 0 if this network accepts anonymous roaming.

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

|  |  |  |
| --- | --- | --- |
| **Credential Category** | **Venue group code** | **Venue type code** |
| **Unspecified Misc entities** | **12** | **0** |
| **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***

Subclause: SLA ANQP-Element

The Service Level Agreement (SLA) ANQP-element provides the STA with information about the type of roaming supported by the ESS, 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 two supported roaming settlement types, the SLA provided by the venue for each type, and optionally details on the venue SLA. The format of the Venue SLA Policy subfield is shown in Figure XX.

****

Figure XX – Venue SLA Policy subfield format

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

The SLA Details field is an optional UTF-8 string 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**  |

**To editors: insert at the end of table 9-331:**

|  |  |  |
| --- | --- | --- |
| **ANQP-element name**  | **InfoID** | **ANQP-element (subclause)** |
| **Credential Types** | **284** | **XX** |
| **SLA** | **285** | **XX** |
| Reserved | ~~284~~**286** – 56 796 | --  |

**To editors: insert at the end of table 11-14:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ANQP-element name**  | **ANQP-element (subclause)** | **ANQP-element type** | **BSS/AP** | **BSS non-AP** | **IBSS /STA** |
| **Credential Types** | **XX** | **S** | **T** | **R** | **--** |
| **SLA** | **XX** | **S** | **T** | **R** | **--** |

**To editors: insert after 11.22.3.3.17:**

Some networks advertise support for multiple SSPs, for example through a RCOI. However, the venue may only accept credentials from subset categories of the RCOI members. In other scenarios, the venue may have specific constraints on the type of credentials that are acceptable, for example based on the identity verification conducted at the credential creation, or the age of the credentials. The Credential Types ANQP-element is used by a non-AP STA to discover the venue requirements for accepted credentials, which includes the SSP categories that are accepted, and the type of validation and age required for the accepted credentials.

The authentication will then occur between the non-AP STA and the SSP through a protected tunnel. In some cases, the local venue requires the non-AP STA to also share locally a contactable identity. The Privacy Indicator field in the Credential Types ANQP-element provides an indication on the venue requirements for contactable identity. Clarifying this requirement allows the STA to preserve the user privacy when identity exposure is not needed.

In some venues, a subset of SSP credentials may not be accepted, for example because they are local competitors. The Excluded NAI Realm provides a list of Realms which credentials are not accepted locally.

When multiple credentials are accepted, the local venue may have specific agreements SSPs based on the roaming profile. The SLA ANQP-element provides the STA with information about the SLA loically available based on the roaming type (free or paid roaming service).

**To editors: insert after bullet 4) in R.2.2:**

5) Credential Types ANQP-element present containing two Credential Types subfields, the first indicating Category Group = 12, Category Type = 1 (Service Provider), Validation = 2 (email, SMS, Government ID or Government issued credentials), Lifetime = 0 (account has been in existence for any duration) and Privacy Indicator = 1 (contactable identity required), the second indicating Category Group = 12, Category Type = 2 (Cloud or Social Media Provider), Validation = 4 (Government ID or Government issued credentials), Lifetime = 4 (account has been in existence for one year or more) and Privacy Indicator = 1 (contactable identity required).

6) SLA ANQP-element present containing First Settlement Indicator = 1 (free services), First SLA Indicator = 1 (Bronze), Second Settlement Indicator = 2 (paid services), Second SLA Indicator = 2 (Silver).

*7~~5~~) There is no RSNE present in the received Beacon frame.*

**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***

Subclause: 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 Excluded NAI Realm Tuple subfields.

The format of an 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 2 plus the length of the Excluded NAI Realm subfield.

The Excluded NAI Realm Encoding subfield uses the same format as the NAI Realm Encoding 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 contains one or more Excluded NAI Realm subfields, which use the same format as the NAI Realm subfield defined in 9.4.5.10.

**To editors: insert at the end of table 9-331:**

|  |  |  |
| --- | --- | --- |
| **ANQP-element name**  | **InfoID** | **ANQP-element (subclause)** |
| **Excluded NAI Realm** | **286** | **XX** |
| Reserved | ~~284~~**287** – 56 796 | --  |

**To editors: insert at the end of table 11-14:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ANQP-element name**  | **ANQP-element (subclause)** | **ANQP-element type** | **BSS/AP** | **BSS non-AP** | **IBSS /STA** |
| **Excluded NAI Realm** | **XX** | **S** | **T** | **R** | **--** |

**To editors: modify R.2.3 as follows:**

A shopper visits a shopping mall and wants to use a smartphone to discover items on sale. In this mall, the mall’s IT department is providing WLAN facilities for all of the stores in the mall; therefore, there is only one SSID for shoppers (i.e., there is not a different SSID for each store in the mall). The user arrives at the mall and taps an icon on the screen to put the smartphone in “shopping mode.” The smartphone’s shopping application causes the non-AP STA to carry out the following steps:

1. a)  The smartphone’s non-AP STA performs an active scan by transmitting a Probe Request frame containing the wildcard SSID and an Interworking element with Access Network Type subfield set to “Free Public Network.” In response, it receives Probe Response frames from several of the mall’s APs, but only one SSID is provided, which is “Silicon Valley Mall.” The mall’s APs did not transmit Probe Response frames for the SSIDs “Engineering,” “Deliveries,” and “Janitorial” since their access network type is “Private network.”
2. b)  The Probe Response frame received by the smartphone indicated the following capabilities:
	1. 1)  Extended Capabilities element indicates: AP provides interworking service.
	2. 2)  Interworking element indicates: venue group = 6 (mercantile) and venue type = 4 (shopping mall), Internet = 0 (unspecified).
	3. 3)  RSNE indicates: IEEE 802.1X authentication.
3. c)  Since the AP indicated Interworking service is available, the smartphone’s non-AP STA uses the MLME-GAS.request primitive to invoke GAS to request the Capability List ANQP-element (see 9.4.5.3). In the Capability List ANQP-element, the AP has indicated support for Venue Name**,** ~~and~~ Domain Name **and Excluded NAI Realm**. Subsequent to receipt of the Capability List ANQP-element, the non-AP STA invokes the MLME-GAS.request primitive to retrieve the other ~~two~~ **three** lists.
4. Next, the non-AP STA’s supplicant searches the received Domain Name list to determine whether it has any stored credentials for these domains **and also searches the Excluded NAI Realm list to determine which realm credentials are not accepted**. If ~~so~~ **the non-AP STAs finds accepted credentials**,
	1. 1)  The smartphone autonomously associates to the “Silicon Valley Mall Shopping” SSID and displays the following information:
		1. i)  Venue name: Silicon Valley Mall, 1234 Main Street, Rownhams, CA 98765-1234
		2. ii)  SSID: Silicon Valley Mall
		3. iii)  Venue type: Shopping Mall
	2. 2)  The supplicant autonomously provides the security credentials for the selected domain.
5. e)  Higher layer protocols then download discount coupons being offered for items on sale.