IEEE P802.11
Wireless LANs

|  |
| --- |
| ANQP elements Augmentation Proposal |
| Date: 2021-10-31 |
| 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 several new ANQP elements that would be of use for the Wi-Fi Alliance and federations use cases.

All the changes are related to Draft P802.11REVme D0.3.

|  |  |  |  |
| --- | --- | --- | --- |
| **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** |
| **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** |

**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.

***Modify the tables in the following clause as shown:***

9.4.1.34 Venue Info field (11u)

**Table 9-93 Venue group codes and descriptions**

|  |  |
| --- | --- |
| **Venue group code** | **Venue group description** |
| … | … |
| 11 | Outdoor |
| 12 | Credential |
| 1~~2~~3-255 | Reserved |

**Table 9-94 Venue type assignments**

|  |  |  |
| --- | --- | --- |
| **Venue group code** | **Venue type code** | **Venue description** |
| … | … | … |
| 11 | 7-255 | Reserved |
| 12 | 0 | Unspecified Miscellaneous Entities |
| 12 | 1 | Service Provider |
| 12 | 2 | Cloud or Social Media Provider |
| 12 | 3 | Cable Industry |
| 12 | 4 | Government |
| 12 | 5-255 | Reserved |

***Modify the table in the following clause as shown:***

* + 1. Access Network Query Protocol (ANQP) elements(11u)

**Table 9-404 ANQP-element definitions**

|  |  |  |
| --- | --- | --- |
| **ANQP-element name** | **InfoID** | **ANQP-(Ed)element****(subclause)** |
| … | … | … |
| Local MAC Address Policy | 283 | 9.4.5.29 |
| Credential Types | <283+ANA> | 9.4.5.30 |
| Service Level Agreement | <283+ANA+1> | 9.4.5.31 |
| Excluded NAI Realm | <283+ANA+2> | 9.4.5.32 |
| Reserved | <283+ANA+3> ~~284~~ - 56 796 | - |
| Vendor Specific | 56 797 | 9.4.5.8 |
| Reserved | 56 798 – 65 535 | - |

***Insert the following new subclause, after 9.4.5.29***

**9.4.5.30. Credential Types ANQP-element**

The Credential Types ANQP-element provides a STA with information about the types of credentials accepted via that AP. The format of the Credential Types ANQP-element is shown in Figure 9-1035a.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Info ID | Length | Credential Types Count | Credential Types Tuples |
| Octets: | 2 | 2 | 1 | Mx3 |

**Figure 9-1035a —** **Credential Types ANQP-element format**

***To editor: in figure 9-1035a above, in “Mx3”, “x” is a multiplication glyph.***

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

The Credential Types Count field specifies the number M of Credential Types Tuple subfields.

The Credential Types Tuples subfield contains zero or more Credential Types Tuple subfields.

The format of a Credential Types Tuple subfield is shown in Figure 9-1035b.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Bits: | B0 B7 | B8 B15 | B16 B18 | B19 B22 | B23 |
|  | Category Group | Category Type | Validation | Lifetime | Privacy Indicator |

**Figure 9-1035b - Credential Types Tuple subfield format**

The Category Group and Category Type subfields specify the credential issuer(s) accepted via the AP, mapped to the Venue group code and the Venue type code in Table 9-66, respectively.

The Validation subfield indicates the minimum type of credential validation that must occur for the credentials to be deemed valid. The values of the subfield are defined in Table 9-413a.

**Table 9-413a Validation subfield values**

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

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 AP requires the user to expose a contactable identity to the AP (usually for legal purposes). It is set to 0 if this AP accepts anonymous roaming.

***Insert the following new subclause, after 9.4.5.30***

**9.4.5.31 Service Level Agreement ANQP-Element**

The Service Level Agreement ANQP-element provides a STA with information about the type of roaming supported by the AP, and the service level agreement (SLA) offered by the AP for a given roaming type. The format of the SLA ANQP-element is shown in Figure 9-1035c.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Info ID | Length | Venue SLA Policy Count | Venue SLA Policy Tuples |
| Octets: | 2 | 2 | 1 | variable |

**Figure 9-1035c — Service Level Agreement ANQP-element format**

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

The Venue SLA Policy Count field specifies the number of Venue SLA Policy Tuple subfields.

The Venue SLA Policy Tuples subfield contains zero or more Venue SLA Policy Tuple subfields.

The format of a Venue SLA Policy Tuple subfield is shown in Figure 9-1035d.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Info ID | Length | Indicators | SLA Details |
| Octets: | 2 | 2 | 1 | variable |

**Figure 9-1035d – Venue SLA Policy Tuple subfield format**

The Indicators subfield indicates the roaming services accepted by the venue and their associated SLAs. The format of the Indicators subfield is shown in Figure 9-1035e.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bits: | B0 B1 | B2 B3 | B4 B5 | B6 B7 |
|  | First Settlement Indicator | First SLA Indicator | Second Settlement Indicator | Second SLA Indicator |

**Figure 9-1035e – Venue SLA Policy Tuple subfield format**

The First Settlement Indicator and Second Settlement Indicator subfields each indicate a type of roaming service accepted by the venue. The values of the First Settlement Indicator and Second Settlement Indicator subfields are specified in Table 9-413b

**Table 9-413b Settlement Indicator**

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

The First SLA Indicator and Second SLA Indicator subfields each indicate the SLA that the AP offers for the respective settlement type. The values of the First SLA Indicator and Second SLA Indicator subfields are specified in Table 9-413c and follow the Olympic model defined in IETF RFC 2597 (Appendix).

**Table 9-413c SLA Indicator**

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

If the First SLA Indicator subfield is set to 0, the Second Settlement Indicator and Second SLA Indicator subfields are reserved. Otherwise, the First SLA Indicator and Second SLA Indicator subfields differ, and a nonzero value in the First SLA Indicator subfield takes precedence over a value of 0 in the Second SLA Indicator subfield, for the settlement type indicated by the First SLA Indicator subfield.

The SLA Details subfield is an optional vendor specific UTF-8 string that can be used to indicate 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.

***To editor, insert the following reference to annex A:***

***IETF RFC 2597, Assured Forwarding PHB Group, J. Heinanen, F. Baker, W. Weiss, J. Wroclawski, June 1999***

**9.4.5.32 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 9-1035f.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Info ID | Length | Excluded NAI Realm Count | Excluded NAI Realm Tuples |
| Octets: | 2 | 2 | 1 | variable |

**Figure 9-1035f — 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 Excluded NAI Realm Tuple subfields.

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 9-1035g.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Excluded NAI Realm Data Field Length | Excluded NAI Realm Encoding | Excluded NAI Realm |
| Octets: | 1 | 1 | variable |

**Figure 9-1035g – Excluded NAI Realm Tuple subfield format**

The Excluded NAI Realm Data Field Length subfield is equal to 1 plus the length of the Excluded NAI Realm subfield.

The Excluded NAI Realm Encoding subfield is shown in Figure 9-1035-h.

|  |  |  |
| --- | --- | --- |
| Bits: | B0 | B1 B7 |
|  | Excluded NAI Realm Encoding Type | Reserved |

**Figure 9-1035h – Excluded NAI Realm Encoding subfield format**

The Excluded NAI Realm Encoding Type subfield is set to 0 to indicate that the NAI realm(s) in the Excluded NAI Realm subfield is/are formatted in accordance with IETF RFC 4282. It is set to 1 to indicate that it/they might not be formatted in accordance with IETF RFC 4282.

The Excluded NAI Realm subfield contains one NAI realm formatted as defined in the Excluded NAI Realm Encoding Type subfield.

***Modify the table in the following clause as shown:***

11.22.3.3.1 General

**Table 11-16 — ANQP usage**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ANQP-element name** | **ANQP-(Ed)element****(subclause)** | **ANQP-element type** | **BSS/AP** | **BSS non-AP** | **IBSS****STA** |
| … | … | … | … | … | … |
| Local MAC Address Policy | 9.4.5.29 | S | T | R | - |
| Credential Types | 9.4.5.30 | S | T | R | - |
| Service Level Agreement | 9.4.5.31 | S | T | R | - |
| Excluded NAI Realm | 9.4.5.32 | S | T | R | - |

***Insert the following new subclause, after 11.22.3.3.16:***

**11.22.3.3.17 Credentials and Privacy procedure**

Some networks advertise support for multiple SSPs, for example through a roaming consortium However, the venue might only accept credentials from a subset of the roaming consortium 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 credentials.

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 allowing the STA to preserve the user’s privacy when identity exposure is not needed.

A Credential Types Tuple subfield shall be ignored if the value in the Validation, Category Group and/or Category Type subfield is reserved.

A First or Second Settlement Indicator subfield and the corresponding First or Second SLA Indicator subfield, respectively, shall be ignored if the value in the First or Second Settlement Indicator subfield, respectively, is reserved.

In some venues, a subset of SSP credentials might not be accepted, for example because they are local competitors. The Excluded NAI Realm ANQP-element provides a list of realms from which credentials are not accepted by the AP.

When multiple credentials are accepted, the local venue may have specific agreements with each SSP based on the roaming profile. The SLA ANQP-element provides the STA with information about the SLA locally available based on the roaming type.

NOTE--How the non-AP STA uses the information indicated by the venue is out of scope of the Standard. It is assumed the non-AP STA has a set of local information about credentials that are available, or policies that are acceptable, and proceeds with a connection based on matching this information to the indicated information.

***Insert the following new bullets, after bullet d) in R.2.2, and renumber current bullets e) and f) as f) and g) respectively:***

**R.2.2 Airport**

e) In large federations (where multiple venues may allow for multiple sources of identities) using Roaming Consortium OI, the multi-to-multi relationship makes it difficult for the STA to understand which credentials from which members of the consortium are actually accepted by the venue. Beyond posing restrictions on the source of credentials, the venue may also mandate a level of robustness for these credentials. The credentials may then only be accepted if the entity providing them has validated the user identity reliably. When validation is light, credentials that have been in existence for a long time may be seen as more reliable than credentials that were created very recently. Last, the venue may have legal requirements to receive a contactable identity for each user. Since the AP has advertised a Roaming Consortium OI, the laptop SME invokes the GAS protocol to retrieve the Credential Types ANQP-element:

1 )The AP response indicates, in the Credential Types ANQP-element, 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).

 2) The laptop now knows which credentials types are accepted.

f) Venues accepting several types of credentials may have agreements to provide different level of service for different types of users. These levels of services are usually agreed upon at a large scale (e.g. all members of a federation), and thus use a common naming convention (Gold, Silver, Bronze). Since the AP has advertised a Roaming Consortium OI and support for Service Level Agreement information, the laptop SME invokes the GAS protocol to retrieve the Service Level Agreement ANQP-element. The AP response indicates: First Settlement Indicator = 1 (free services), First SLA Indicator = 1 (Bronze), Second Settlement Indicator = 2 (paid services), Second SLA Indicator = 2 (Silver). The laptop can then select, from the profiles with accepted credentials, those that also accept the SLA offered by the venue.

***Modify the following clause:***

**R.2.3 Shopping**

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:

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.”

b)  The Probe Response frame received by the smartphone indicated the following capabilities:

1)  Extended Capabilities element indicates: AP provides interworking service.

2)  Interworking element indicates: venue group = 6 (mercantile) and venue type = 4 (shopping mall), Internet = 0 (unspecified).

3)  RSNE indicates: IEEE 802.1X authentication.

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~~ lists.

d) Next, the non-AP STA’s supplicant searches the received Domain Name list to determine whether it has any stored credentials for these domains.

e) In some cases, the venue may also not accept credentials from competing entities. Therefore, the non-AP STA’s supplicant also searches the list of excluded NAI realms to determine which realm credentials are not accepted. The non-AP STA discards the credentials that match elements of the exluded NAI realm list returned by the AP. If ~~so~~ the non-AP STAs finds accepted credentials,

1)  The smartphone autonomously associates to the “Silicon Valley Mall Shopping” SSID and displays the following information:

i)  Venue name: Silicon Valley Mall, 1234 Main Street, Rownhams, CA 98765-1234

ii)  SSID: Silicon Valley Mall

iii)  Venue type: Shopping Mall

2)  The supplicant autonomously provides the security credentials for the selected domain.

f~~e~~)  Higher layer protocols then download discount coupons being offered for items on sale.