IEEE P802.11
Wireless LANs

|  |
| --- |
| Hashed Domain Names |
| Date: 2015-10-12 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HP | 1322 Crossman avenue, Sunnyvale, California, United States of America | +1 408 227 4500 | dharkins at aruba networks dot com |
|  |  |  |  |  |

Abstract

This submission addresses CIDs 10037, 10039, 10040, and 10041.

 CID 10037

|  |  |  |  |
| --- | --- | --- | --- |
| CID | Comment | Proposed Change | Proposed Resolution |
| 10037 | Hash Domain Information is not necessary and its use supposes this information is available when, in practice, it is not. | remove the Hashed Domain information from the FILS Request Parameters element, remove the Hashed Domain Information Present bit from the Parameter Control Bitmap field, and remove the Hashed Domain Information field and its accompanying text. | Accept |

***Instruct the editor to modify section 8.4.2.173 as indicated:***

**8.4.2.173 FILS Request Parameters element**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Minimum Data Rate | RCPI Limit | OUI Response Criteria | Max Channel Time |  |

 Octets: 0 or 3 0 or 1 0 or 2 0 or 1

 **Figure 8-577d—FILS Request Parameters element format**

|  |  |  |  |
| --- | --- | --- | --- |
|  OUI Response Criteria Present | Max Channel Time Present |  |  Reserved |

 Bits: 1 1 1 2

 **Figure 8-577e—Parameter Control Bitmap field**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |   |  |

CID 10040

|  |  |  |  |
| --- | --- | --- | --- |
| CID | Comment | Proposed Change | Proposed Resolution |
| 10040 | These are not “Domain Identifiers”, they indicate supported “realms” for EAP-RP. | Reword the “Domain Identifier” portions of this section to indicate supported “realms” for EAP-RP. Don’t indicate “Hashed Domain Names”, indicate hashed realms. | Revised: changed “domain” to “realm” throughout. |

***Instruct the editor to modify section 8.4.2.178 as indicated:***

**8.4.2.178 FILS Indication element**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Element ID | Length | FILS Information | Cache Identifier | RealmIdentifier | Public Key Identifier |

Octets: 1 1 2 0 or 16 variable variable

 **Figure 8-577l—FILS Indication element forma**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Number of Public Key Identifiers | Number of RealmIdentifiers | FILS IP Address Configuration | Cache Supported | Reserved |

 **Figure 8-577m—FILS Information field definition**

The Number of RealmIdentifiers subfield lists the number of realm identifiers that are present in the Realm Identifier field in the FILS Indication element. When the Number of Realm Identifiers subfield is 0, the Realm Identifier field is not present in the FILS Indication element. Each realm identifier is formatted per Figure 8-574n (Realm Identifier entry). Up to seven Realm Identifiers fields may be carried in FILS Indication element.

|  |
| --- |
| Hashed RealmName |

 Octets: 2

  **Figure 8-577n—RealmIdentifier Field**

The value of the Hashed Realm Name subfield of the RealmIdentifier field entry is computed from the realm name that is compliant with the preferred name syntax defined in IETF RFC 1035 (same as the domain name used in 8.4.5.15 (Domain Name ANQP-element)). The exact computation method for the hashed realmname is given in 10.45.4 (FILS authentication and higher layer setup capability indications).

CID 10039

|  |  |  |  |
| --- | --- | --- | --- |
| CID | Comment | Proposed Change | Proposed Resolution |
| 10039 | Get rid of the hash domain name stuff | Remove step 7 | Accept |

***Instruct the editor to modify section 10.1.4.3.4 as indicated:***

**10.1.4.3.4 Criteria for sending a ~~probe~~ response**

A FILS STA shall not respond to a Probe Request frame if any of the following criteria is met for a FILS Request Parameters element contained in the Probe Request frame:

CID 10041

|  |  |  |  |
| --- | --- | --- | --- |
| CID | Comment | Proposed Change | Proposed Resolution |
| 10041 | This section should be only about hashing of realms, not domain names | reword section to say that the AP is indicating 8 realms for which it can offer EAP-RP support. Remove the option for "D" in the calculations that indicates "Home network". | Revised: text indicates “realms” per RFC 6966 |

***Instruct the editor to modify section 10.74.4 as indicated:***

**10.74.4 FILS authentication and higher layer setup capability indications**

A FILS AP shall include a FILS Indication element in Beacon and Probe Response frames, and may include a FILS Indication element in FILS Discovery frames. The FILS Indication element indicates properties of the FILS authentication protocol used, whether the AP performs IP address assignment, and the IP address type.

An AP can indicate up to 7 realms that indicate the domain name of the ER server that the AP is capable of participating in an EAP-RP exchange with (see RFC 6966). . The realm name of an ER server is the realm portion of the keyName-NAIas defined in IETF RFC 6696. For each of the realmnames, the FILS Indication element carries a 2-octet hash of the network realmname and the IP address type of the corresponding domain. The hash of the realm name (IETF RFC 1035 compliant) is computed as follows:

NOTE— Internationalized domain names are first converted to an IETF RFC 1035 compliant ASCII form using the

operations defined in IETF RFC 3490.

 H = L(CRC32-(x),0,16),0,15) (2)

where:

CRC-32(x) is calculated by using G(x) function defined in 8.2.4.8 (FCS field), where x is ToLower-Case(D)

H is the hashed realmname,

L is defined in 11.6.1,

ToLowerCase is the function that converts upper case characters to lower case

D is: NAI Realm of the ER server used in EAP-RP authentication.

**References:**