IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolution of CID 8020 from LB213 | | | | |
| Date: 2016-06-30 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman avenue, Sunnyvale, California, United States of America | +1 408 227 4500 | dharkins at aruba networks dot com |
|  |  |  |  |  |

Abstract

This submission proposes a resolution to CID 8020 from LB213.

***Instruct the editor to modify section 11.11.2.2 as indicated:***

**11.11.2.2 Discovery of a FILS capable AP**

An AP indicates that it is capable of performing FILS authentication by indicating support for a FILS AKM in an RSN element and including it, and the FILS Indication element, in Beacons and Probe Response frames.

An AP may indicate that it is capable of performing FILS authentication by indicating support for a FILS AKM in the FD RSN subfield in a FILS Discovery frame.

An AP indicates support for shared key authentication by advertising between zero and seven realms using a Domain Information subfield of the FILS Indication element that is part of Beacon, Probe Response, and FILS Discovery frames. If the STA discovers a FILS-capable AP that advertises a hashed domain name that matches the hashed value of the realm of the third party Authentication Server, with which the STA shares a valid rRK as defined in IETF RFC 6696, the STA may begin the FILS authentication protocol with the AP using EAP-RP. Domain name hashing is specified in 10.47.4 (FILS authentication and higher layer setup capability indications). If a STA discovers a FILS-capable AP that does not advertise any realms, or that advertises realms unknown to the STA, and the STA believes it shares a PMKSA with the AP, it may begin the FILS authentication protocol with the AP using PMKSA caching.

**References:**