IEEE P802.11
Wireless LANs

|  |
| --- |
| Element Validation  |
| Date: 2014-09-10 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman avenue, Sunnyvale, CA, 94089 | +1 408 227 4500 | dharkins at aruba networks all one word dot com |
|  |  |  |  |  |

Abstract

The text on how to validate elements for both ECC and FFC groups is in text specific to processing of certain 802.11 Authentication frames. By moving it into the general sections on ECC and FFC groups it makes it possible to refer to by other protocols that use these groups instead of requiring the other protocols to repeat this text in the section specific to the processing of its frames.

***Instruct the editor to modify section 11.3.4.2.1 as indicated:***

**11.3.4.2.1 ECC group definition**

ECC groups used by SAE are defined by the sextuple (p, a, b, G, r, h) where p is a prime number, a and b

specify the elliptic curve defined by the equation, y2 = x3 + ax + b modulo p , G is a generator (a base point on the elliptic curve), r is the prime order of G , and h is the co-factor. Elements in ECC groups are the points on the elliptic curve defined by their coordinates—(x, y)—that satisfy the equation for the curve and the identity element, the so-called “point at infinity.

ECC elements are validated by ensuring that both the x- and y- coordinates of the element are non-negative numbers less than the prime number p, and that the two coordinates produce a valid point on the curve satisfying the group’s curve definition, not being equal to the “point at infinity”. If either of these conditions do not hold, the element is not valid.

***Instruct the editor to modify section 11.3.4.3.1 as indicated:***

**11.3.4.3.1 FFC group definition**

FFC groups used by SAE are defined by the triple (p , G , r ), where p is a prime number, G is a generator, and r is the prime order of G modulo p . An element, B, in an FFC group satisfies B = Gi  modulo p for some integer i . This special property differentiates elements from scalars, even though both elements and scalars can be represented as non-negative integers less than the prime modulus p. The notation convention of 11.3.4 (Finite cyclic groups) signifies this difference between an element and a scalar in an FFC group. The identity element for an FFC group is the value one (1) modulo p .

FCC elements are validated by ensuring that the element is an integer greater than one (1) and less than the prime number p, and that the scalar operation of the element and the order of the group, r, is equal to one (1) modulo the prime number p. If either of these conditions do not hold, the element is not valid.

***Instruct the editor to modify section 11.3.5.4 as indicated:***

**11.3.5.4 Processing of a peer’s SAE Commit message**

If the scalar value is greater than zero (0) and less than the order, r , of the negotiated group, scalar validation succeeds; otherwise, it fails. Element validation depends on the type of group. For FFC groups,element validation is specified in 11.3.4.3.1 (FFC group definition). . For ECC groups, element validation is specified in 11.3.4.2.1 (ECC group definition).

If either scalar validation or element validation fails, the STA shall reject the peer’s authentication.

**References:**