IEEE P802.11
Wireless LANs

|  |
| --- |
| Support for Internationalized Character Sets |
| Date: 2020-03-12 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Smith Kennedy | HP Inc |  |  |  |
| Mike Montemurro  | Blackberry |  |  |  |
| Dan Harkins | HP Enterprise |  |  |  |

Abstract

This submission proposes the use of character pre-processing methods in order to support internationalized character sets with usernames (password identifiers) and passwords.

**Discussion**: Currently, SAE defines a password as an ASCII string while the MIB entry it uses to retrieve that string says the password is an OCTET-STRING. IEEE 802.11 is an international standard and as such needs to support international character sets. Some international character sets, unfortunately, have non-unique ways of representing some characters, an ambiguity that can cause two sides to enter identical passwords but end up having different binary representations. Therefore the SAE password and password identifier need to be processed using profiles defined in RFC 8265 prior to storing the octet strings in the MIB (which is also prior to beginning SAE).

*Instruct the editor to modify section 2 as indicated:*

IETF RFC 8200, Internet Protocol, Version 6 (IPv6) Specification, S. Deering, R. Hinden, 2017.

IETF RFC 8265, Preparation, Enforcement, and Comparison of Internationalized Strings Representing Usernames and Passwords, P. Saint-Andre, A. Melnikov, 2017.

ISO 639, Codes for the Representation of Names of Languages.

*Instruct the editor to modify section 12.4.3 as indicated:*

**12.4.3 Representation of a password**

Passwords are used in SAE to deterministically compute a secret element in the negotiated group, called a password element. The input to this process needs to be in the form of a binary string. For the protocol to successfully terminate, it is necessary for each side to produce identical binary strings for a given password, even if that password is in character format. There is no canonical binary representation of a character and ambiguity exists when the password is a character string. To eliminate this ambiguity, a STA shall represent a character-based password as a UTF-8 string that is processed according to the OpaqueString profile of IETF RFC 8265, the output of which is an octet string.The octet string representation of the password, after being processed, is stored in the dot11RSNAConfigPasswordValueTable. When a “password” is called for in the description of SAE that follows the credential from the dot11RSNAConfigPasswordValueTable is used.

Similarly, to address ambiguity when identifying passwords, a STA shall represent a password identifier as a UTF-8 string that is processed according to the UsernameCasePreserved profile of IETF RFC 8265, the output of which is an octet string that is stored in the dot11RSNAConfigPasswordValueTable. When a “password identifier” is called for in the description of SAE that follows, the identifier from the dot11RSNAConfigPasswordValueTable is used.

In an infrastructure BSS for which an SAE AKM is indicated, the AP shall set the SAE Password Identifiers In Use subfield of the Extended Capabilities field of the Extended Capabilities element to 1 if any entry in the dot11RSNAConfigPasswordValueTable has a non-NULL dot11RSNAConfigPasswordIdentifier, and shall set it to 0 otherwise. Similarly, an AP shall set the SAE Password Identifiers Used Exclusively subfield of the Extended Capabilities field of the Extended Capabilities element to 1 if every entry in the dot11RSNAConfigPasswordValueTable has a non-NULL dot11RSNAConfigPasswordIdentifier and shall set it to 0 otherwise.

*Instruct the editor to modify Annex C as indicated:*

dot11RSNAConfigPasswordCredential OBJECT-TYPE SYNTAX OCTET STRING
 MAX-ACCESS read-write

 DESCRIPTION

 "This is a control variable.
 It is written by an external management entity.
 Changes take effect as soon as practical in the implementation.

 This variable is an octet string representation of a shared, secret, and potentially low entropy word, phrase, code or key used as an authentication credential.

 Any character-based word or phrase shall be converted
 into a canonical representation according to
 12.4.3 (Representation of a password) before populating the Password Credential."

::= { dot11RSNAConfigPasswordValueEntry 2 }

dot11RSNAConfigPasswordIdentifier OBJECT-TYPE SYNTAX OCTET STRING
 MAX-ACCESS read-write
 STATUS current

 DESCRIPTION
 "This is a control variable.
 It is written by an external management entity.
 Changes take (Ed)effect as soon as practical in the implementation. This variable is an octet string that an implementation uses to uniquely identify a password to support provisioning multiple passwords for
a single peer MAC entity. It shall be converted into a canonical representation according to 12.4.3 (Representation of a password) before populating the Password Identifier."

::= { dot11RSNAConfigPasswordValueEntry 3 }

**References:**