|  |  |
| --- | --- |
| Project | **IEEE 802.21d****<https://mentor.ieee.org/802.21>** |
| Title |  **Security text for Multicast Group Management** |
| DCN | **21-13-** |
| Date Submitted |  |
| Source(s) | Lily Chen, Karen Randall |
| Re: |  |
| Abstract | This contribution proposes changes to support the use of ECDSA and clarifies the use of AES-CCM. |
| Purpose | Proposed text to resolve comments 219 and 220 |
| Notice | This document has been prepared to assist the IEEE 802.21 Working Group. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE’s name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE’s sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that IEEE 802.21 may make this contribution public. |
| Patent Policy | The contributor is familiar with IEEE patent policy, as stated in [Section 6 of the IEEE-SA Standards Board bylaws](http://standards.ieee.org/guides/opman/sect6.html#_blank) <[http://standards.ieee.org/guides/bylaws/sect6-7.html#6](http://127.0.0.1:4664/cache?event_id=757737&schema_id=1&s=5X0vID10lu_E6yrIkWkNd4Wz2H8&q=hancock#_blank)> and in *Understanding Patent Issues During IEEE Standards Development* [http://standards.ieee.org/board/pat/faq.pdf](http://standards.ieee.org/board/pat/faq.pdf#_blank) |

Insert the following references to Clause 2, Normative References

IEEE Std 802.1AR™-2009, IEEE Standard for Local and Metropolitan Area Networks: Secure Device Identity.

QUESTION - The following references are normative in IEEE 802.1AR but they could be included in the bibliography here. The question for the 21d document – is IEEE 802.1AR sufficient as the normative reference, or do the normative references in AR need to be normative in 21d too? Any preference?

ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).1

IETF RFC 5008, Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME), Housley, R., Solinas, J., September 2007.2

IETF RFC 5480, Elliptic Curve Cryptography Subject Public Key Information, Turner, S., Brown, D., Yiu, K., Housley, R., Polk, T., March 2009.

NIST FIPS 186-4, Digital Signature Standards (DSS), July 2013.3

1ANSI publications are available from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (<http://www.ansi.org/>).

2IETF RFCs are available from the Internet Engineering Task Force Web site at http://www.ietf.org/rfc.html.

3NIST publications are available from the National Institute of Standards and Technology, NIST Public Inquiries, NIST, 100 Bureau Drive, Stop 3460, Gaithersburg, MD, 20899-3460, USA (www.nist.gov).

Suggest to insert the following text after the first paragraph of Clause 9.4.5.

In this specification, Elliptic Curve Digital Signature Algorithm (ECDSA) specified in FIPS 186-4 is used as the multicast signature scheme. In particular, NIST recommended elliptic curve P-256, specified in FIPS 186-4 and hash function SHA-256 specified in FIPS 180-4 are used to generate signatures. The algorithm identifiers are introduced in Clause 9.4.5.4.

Insert the following clause:

9.4.5.4 Algorithm identifiers

The ECDSA signature method is defined in IEEE 802.1AR-2009, Secure Device Identity, by reference to NIST FIPS 186-4 and ANSI X9.62-2005.

If implementing ECDSA P-256, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be ecdsa-with-SHA256 as specified in IEEE 802.1AR by reference to RFC 5008. The object identifier is:

ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-sha2(3) 2 }

When the ecdsa-with-SHA256 algorithm identifier appears in the algorithm field as an AlgorithmIdentifier, the encoding shall omit the parameters field. That is, the AlgorithmIdentifier shall be a SEQUENCE of one component, the object identifier ecdsa-with-SHA256.

QUESTION: should we include reference info for the subjectPublicKeyInfo for the certificate?

The algorithm identifier for ECDSA signature keys to be used in an X.509 certificate is specified in IEEE 802.1AR and RFC 5480 as id-ecPublicKey:

id-ecPublicKey OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-x9-62(10045) keyType(2) 1 }

ECDSA requires the use of certain parameters with the public key for the X.509 certificate. As specified in RFC 5480 the parameter structure is:

ECParameters ::= CHOICE {

namedCurve OBJECT IDENTIFIER

-- implicitCurve NULL

-- specifiedCurve SpecifiedECDomain

}

The namedCurve choice, which allows all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier, shall be used. The object identifier for the P-256 curve is:

ansip256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-x9-62(10045) curves(3) prime(1) 7 }

The ECDSA public key is as specified in RFC 5480 and included here for convenience:

ECPoint ::= OCTET STRING

Implementations shall support the uncompressed form and may support the compressed form of the ECDSA public key. The hybrid form of the ECC public key from ANSI X9.62-2005 shall not be used.

Suggest inserting the following text after Table 26 in Clause 9.4.6.

In Table 26, AES-CCM is an AES mode of operations specified in NIST SP 800-38C. AES-CCM provides confidentiality and data integrity.

In Table 26, ECDSA-256 uses curve P-256 and hash function SHA-256.

*(Note remove entries in table 26 that reference/use ECDSA-224).*

Notice that AES-CCM uses the group key, either MIGMEK or MIGEK. It can provide data integrity but not unique data origin authentication because the symmetric key is shared among a group of MNs. The data origin authentication is provided through ECDSA.

The data protection procedure is illustrated in Figure xxx.

*[include figure to illustrate the AES-CCM and signature.]*