CRITERIA FOR STANDARDS DEVELOPMENT (CSD) for a proposed PAR:

P802.1ARce
IEEE Standard for Local and metropolitan area networks –
Secure Device Identity –
Amendment 1: SHA-384 and P-384 Elliptic Curve

The text of the CSD given here in italics is that provided on the IEEE 802 website under 'IEEE 802 Procedural Documents' based on IEEE 802 LMSC Operations Manuals approved 15 November 2013 and last edited 20 January 2014. Responses to the questions asked in the CSD are given in roman font.

1. IEEE 802 criteria for standards development (CSD)

The CSD documents an agreement between the WG and the Sponsor that provides a description of the project and the Sponsor's requirements more detailed than required in the PAR. The CSD consists of the project process requirements, 1.1, and the 5C requirements, 1.2.

1.1 Project process requirements

1.1.1 Managed objects

Describe the plan for developing a definition of managed objects. The plan shall specify one of the following:

- *a) The definitions will be part of this project.*
- *b) The definitions will be part of a different project and provide the plan for that project or anticipated future project.*
- *c) The definitions will not be developed and explain why such definitions are not needed.*

Definition of managed objects in the form of an SNMP MIB is part of IEEE 802.1AR. If this amendment to IEEE 802.1AR results in changes that need to be accompanied by changes to the definition of managed objects then those changes will be developed as part of this project.

1.1.2 Coexistence

A WG proposing a wireless project shall demonstrate coexistence through the preparation of a Coexistence Assurance (CA) document unless it is not applicable.

- *a) Will the WG create a CA document as part of the WG balloting process as described in Clause 13? (yes/no)*
- *b) If not, explain why the CA document is not applicable.*

This is not a wireless project so a Coexistence Assurance (CA) document is not applicable.

1.2 5C requirements

1.2.1 Broad market potential
Each proposed IEEE 802 LMSC standard shall have broad market potential. At a minimum, address the following areas:

a) Broad sets of applicability.
b) Multiple vendors and numerous users.

This amendment is applicable to all networks that are currently using or planning to use IEEE 802.1AR, Secure Device Identity. The addition of these options that provide additional cryptographic strength will broaden the applicability of IEEE 802.1AR to appeal to those customers desiring the use of the stronger security (i.e., 192 bits).

1.2.2 Compatibility

Each proposed IEEE 802 LMSC standard should be in conformance with IEEE Std 802, IEEE 802.1AC, and IEEE 802.1Q. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with IEEE 802.1 WG prior to submitting a PAR to the Sponsor.

a) Will the proposed standard comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q?
b) If the answer to a) is no, supply the response from the IEEE 802.1 WG.

The review and response is not required if the proposed standard is an amendment or revision to an existing standard for which it has been previously determined that compliance with the above IEEE 802 standards is not possible. In this case, the CSD statement shall state that this is the case.

The amendment will be in conformance with IEEE Std 802, IEEE Std 802.1AC, and IEEE 802.1Q. It will fit within the framework provided by IEEE 802.1AR-2009.

1.2.3 Distinct Identity
Each proposed IEEE 802 LMSC standard shall provide evidence of a distinct identity. Identify standards and standards projects with similar scopes and for each one describe why the proposed project is substantially different.

IEEE 802.1AR is already a recognized and established standard, applicable to security not covered by other 802 standards and currently lacking support for the SHA-384 hash and P-384 elliptic curve.

1.2.4 Technical Feasibility
Each proposed IEEE 802 LMSC standard shall provide evidence that the project is technically feasible within the time frame of the project. At a minimum, address the following items to demonstrate technical feasibility:

a) Demonstrated system feasibility.
b) Proven similar technology via testing, modeling, simulation, etc.

The characteristics of P-384 and SHA-384 are already well known. Both have been referenced in RFC 5759 and are also anticipated to be included in the updated TPM 2.0 specification from the Trusted Computing Group. Technology for testing cryptographic modes of operations is well advanced. SHA-384 and P-384 elliptic curve has been adopted by NIST.

1.2.5 Economic Feasibility
Each proposed IEEE 802 LMSC standard shall provide evidence of economic feasibility. Demonstrate, as far as can reasonably be estimated, the economic feasibility of the proposed project for its intended applications. Among the areas that may be addressed in the cost for performance analysis are the following:

a) Balanced costs (infrastructure versus attached stations).
b) Known cost factors.
c) Consideration of installation costs.
d) Consideration of operational costs (e.g., energy consumption).
e) *Other areas, as appropriate.*

The economic factors for adoption of this technology outweigh the estimated costs of implementing the solution. Experience with cryptography providing 192 bits of strength has met customer needs for cost of perceived value. No differences in installation costs are expected. No changes in installation practice are anticipated.