IEEE 802 LAN/MAN STANDARDS COMMITTEE (LMSC)

CRITERIA FOR STANDARDS DEVELOPMENT (CSD)

Based on IEEE 802 LMSC Operations Manuals approved 17 March 2022
Last edited 20 May 2025

IEEE P802.1AReg Amendment: Support for the Module-Lattice-Based Digital Signature Algorithm.

1. IEEE 802 criteria for standards development (CSD)

The CSD documents an agreement between the WG and the LMSC that provides a description of the project and the LMSC'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.

1.1.1 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.

Item c) applies:

The MIB currently in IEEE 802.1AR-2018 applies independently from the signature suite, each suite being allocated a simple identifier. So the MIB module does not need to be updated to support the amended function. Further additions to the MIB are undesirable as they could be useful to attackers.

The RFC 9642 titled “A YANG Data Model for a Keystore” already covers IEEE Std 802.1AR as explicitly stated in the third paragraph of Clause 1 of RFC 9642.

RFC 9642 does not require particular Signature Suites to be built into the YANG, so does not need to be updated as new cryptographic algorithms are used and therefore is applicable to ML-DSA without any modification.

RFC 9642 includes introductory material ("1.1 Relation to Other RFCs") that explains the relationship between RFCs 9640 to 9645 and Internet Drafts for YANG modules that cover the

related subjects of crypto-types, truststore, keystore, tcp-client-server, ssh-client-server, tls-client-server, http-client-server, netconf-client-server, and restconf-client-server.

1.1.2 Coexistence: N/A

A WG proposing a wireless project shall prepare a Coexistence Assessment (CA) document unless it is not applicable.

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

Item e) applies since this is not a wireless project.

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:

f) Broad sets of applicability.
g) Multiple vendors and numerous users.

The IEEE Std 802.1AR has been widely deployed. The development of quantum computing poses a threat that might break the current device identifiers specified in IEEE Std 802.1AR-2018. These device identifiers are used to secure a broad range of devices including networking switches, routers, host computers, and network-attached appliances. In the near-term governments are requiring quantum safe cryptographic algorithms for new procurements. In the longer term all sensitive devices will need support for quantum safe device identification. We already have multiple vendors preparing device identification solutions to meet the market demand.

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.

h) Will the proposed standard comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q?
i) 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.

This standard will comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q.

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.

No projects have a similar scope to the proposed project. Other projects such as those at Trusted Computing Group (TCG) are dependent on this work.

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:

j) Demonstrated system feasibility.
k) Proven similar technology via testing, modeling, simulation, etc.

The proposed cryptographic algorithm additions have been thoroughly researched by the National Institute of Standards and Technology (NIST) which has published the specification in FIPS 204.

Many software implementations currently exist. The transition to hardware does not appear to present novel problems.

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:

l) Known cost factors.
   The DevIDs are typically contained in Trusted Platform Modules (TPM). The ML-DSA capable modules will require more memory in the order of 100s Kbytes – Mbytes since the ML-DSA key sizes are about 8x larger than the current keys, however are not expected to be significantly more expensive than the current TPM devices since the TPM will still be a single chip with the packaging being the most important cost factor.
m) Balanced costs.
   The cost of TPMs is typically insignificant vs the total cost of the switch, server, or computer containing the TPM.
n) Consideration of installation costs.
   The DevIDs are typically implemented in a TPM which is a pluggable module and so can be upgraded by swapping the TPM for a TPM supporting ML-DSA.
o) Consideration of operational costs (e.g., energy consumption).

The added memory for the ML-DSA TPM typically adds an insignificant amount of energy consumption relative to the total system.

p) Other areas, as appropriate.