MAC Data Security

Study Group Formation

Mick Seaman 15 SEPT 2026

MAC Data Security

Study Group formation

Approve the formation of 802.1 MAC Data Security Study Group to consider the development of a Project Authorization Request (PAR) and Criteria for Standards Development (CSD) responses for an amendment to IEEE Std 802.1AE Media Access Control (MAC) Security a.k.a “MACsec” or a new 802.1 Standard (as determined by the Study Group) to protect data where the underlying transport does not preserve the MAC Addresses of the communicating peers.

See following slide(s) and
https://www.ieee802.org/1/files/public/docs2026/new-seaman-mac-data-security-0526-v00.pdf
for supporting documentation.

Vote in the WG: Y __ N__ A__

MAC Data Security

Anticipated scope (brief) of the proposed amendment or new standard

Specification of additional Cipher Suites to provide data integrity, optional confidentiality, data origin authenticity, and replay protection without requiring communicating peers to use the same DA & SA MAC addresses. The additional Cipher Suites (will) use the existing IEEE Std 802.1AE concepts and SecTAG, and existing Authenticated Encryption with Associated Data (AEAD) cryptography (GCM/Ascon).

Guidance/specification of the use of specific protocols to transport the protected data between authenticated peers.

NOTE: Transport protocols can prepend and remove unprotected data and identifiers, potentially modified en-route between the authenticated peers, as (for example) is done by Ethernet Data Encryption devices (EDEs, Clause 15 of IEEE Std 802.1AE-2018). Identification of potentially useful transport/protocols scenarios should be part of Study Group activity.

MAC Data Security

Need (as currently expressed)

Extension of the current MACsec performance and protection capabilities to provide ‘end-to-end’ protection, where those ‘end’s typically represent the extent of the responsibility of a single provider organization that can be providing part of the overall application communication path.

NOTE—‘Virtual LAN over Cloud’ scenarios where the entire original frame (DA, SA, and Data) is communicated peer-to-peer are already supported by existing MACsec. However that protection cannot localize attacks/faults to specific path segments in the core of the network, and will use data keys that are not available (by design) to equipment on path.

MAC Data Security

Scope constraints

In: Use of CAK (pairwise symmetric master key, PSK or 802.1X) and existing MKA for SAK distribution and roll-over. Retain means outside the standard for CAK/PSK distribution.

Out: Specification of new authentication methods for CAK generation or new key agreement (SAK distribution) methods beyond 802.1X MKA.

In: Specification or guidance for particular transports and their protocol identification.

Out: Extension or modification of Cipher Suite to cover transport fields.

In (must have): MAC Privacy protection

MAC Data Security

Risks: Scale

Implementation needs rapid (per frame) access to per SA expanded data key (SAK) schedules and data (nextPN etc.) and per SC (secure channel) statistics.

MACsec very deliberately protected all transmitted traffic through a port using a single SC, with only two SAs concurrent for roll-overs. Received traffic uses a single SC per peer, with only two SAKs for all peers (including transmit).

Current implementations can support many ports with more (~256+?) SCs.

Limits may be OK for provider trunk paths in the core and network edges near customers, but well short of per customer protection in the core.

NOTE: