

IEEE 1722.1

Counter names, Encryption key types, and MACsec support

Jeff Koftinoff <jkoftino at ford dot com>

Working group review · 5 August 2026

PROPOSAL 1

GET_COUNTERS_NAMES

New AECp AEM command — proposed 7.4.77. Returns a localized name for every counter slot of a given descriptor.

WHY

- Entity-specific counter slots are opaque: a generic controller has no interoperable way to show what a vendor counter means.

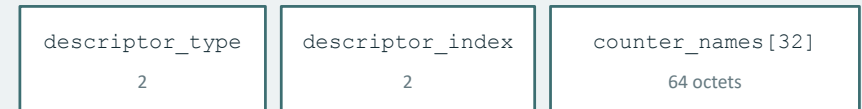
HOW

- A dedicated command — descriptors are not extended, so the static descriptor set and the on-wire model are unchanged.
- Exactly 32 `localized_string_reference` values, one per counter slot, in counter-index order (bit 0 → slot 0).
- Resolves through the existing `LOCALE` / `STRINGS` descriptors
- Support is discovered by issuing the command: unsupported entities respond with status `NOT_IMPLEMENTED`.
- If the requested descriptor does not have counters, the returned status is `NOT_SUPPORTED`

COMMAND PDU



RESPONSE PDU



0xFFFF (`NO_STRING`) marks an unnamed or reserved slot.

Applies to: `ENTITY` · `AVB_INTERFACE` · `CLOCK_DOMAIN` · `STREAM_INPUT`
· `STREAM_OUTPUT`

Open `command_type` value (0x0069 used as a placeholder)

PROPOSAL 2

New key types for the key catalogue

Table 7-181 (7.6.1.2).

Key type	Identifier	Key length (octets)	Description
X25519_PUBLIC	4	32	Raw X25519 public key used for ECDH key agreement
X25519_PRIVATE	5	32	Raw X25519 scalar
ED25519_PUBLIC	6	32	Ed25519 public key
ED25519_PRIVATE	7	32	Ed25519 private key
AES_SIV_128	8	32	AES-SIV-128 session key with 256 bits of keying material - two independent 128-bit keys (S2V + CTR)
AES_SIV_256	9	64	AES-SIV-256 session key with 512 bits of keying material - two independent 256-bit keys (S2V + CTR)
MACSEC_SAK_128	10	16	Secure Association Key for GCM-AES-128 / XPN-128
MACSEC_SAK_256	11	32	Secure Association Key for GCM-AES-256 / XPN-256

Signature representation

AUTH_GET_IDENTITY (7.4.63) returns `ecdsa_signature_c / _d`; these become a single 64-octet `signature_value`, as in Clause 16. The `key_id` field identifies the manufacturer's verification key, and its `key_type` determines how the field is interpreted: `c || d` for `ECC_PUBLIC_256`, an RFC 8032 signature for `ED25519_PUBLIC`. 7.6.5 needs an Ed25519 signing procedure alongside the existing 1363a/EMSA1/SHA-256 one.

Key chains (Table 7-184)

`ENTITY_*`, `MANUFACTURER_PUBLIC`, `CONTROLLERS` and `TRANSPORT` name `ECC_*_256` explicitly. Update them to allow the 25519 types, let `TRANSPORT` carry AES-SIV, and add a MACSEC chain for SAKs.

PROPOSAL 2 (cont.)

Commands for Controller-driven SAK rotation

Four new MACsec commands. Key delivery and fault notification reuse existing mechanisms, unchanged.

Command	Command fields	Response
AUTH_MACSEC_INSTALL_SA	interface_index, sci, an, key_id, cipher_suite, lowest_acceptable_pn, flags (RX / TX)	echo + status
AUTH_MACSEC_SET_TX_SA	interface_index, sci, an	echo + status
AUTH_MACSEC_DELETE_SA	interface_index, sci, an	echo + status
AUTH_MACSEC_GET_SA_STATUS	interface_index, sci	per AN: key_id, flags (installed / rx / tx-active), next_pn, validated + invalid frame counts
unsolicited notification <i>existing — no change</i>	—	SA down, validation failure, PN threshold reached

sci — Secure Channel Identifier, 64 bits: a 48-bit MAC address concatenated with a 16-bit Port Identifier.

an — Association Number, 2 bits, values 0–3, carried in the SecTAG of every protected frame.

cipher_suite — 802.1AE 64-bit cipher suite identifier

lowest_acceptable_pn — 64 bit value for replay protection.

MAKE-BEFORE-BREAK USES EACH ONE EXACTLY ONCE

- 1 deliver to both peers → AUTH_ADD_KEY_NONCE
- 2 install under next AN, RX only → AUTH_MACSEC_INSTALL_SA
- 3 ready-gate — confirm both ends → AUTH_MACSEC_GET_SA_STATUS
- 4 switch TX → AUTH_MACSEC_SET_TX_SA
- 5 retire old AN → AUTH_MACSEC_DELETE_SA

SAK bytes are never readable. Status returns key_id only, tying an SA to a delivered key.

Install must be idempotent. AECP retransmits on timeout; a repeat must not disturb a live SA.