ONEDGE ENERGY

BMS-TEE Attestation Chain Specification

TEEATTEST-1.0.0

Normative; under STANDARD axis S-0.0.4

Issuer:	IKKUNA SpA (StandardCo)
Document Type:	Normative attestation-chain specification
Version:	TEEATTEST-1.0.0
Parent:	S-0.0.4 (Hardening Note v0.0.4); references GRSCHEMA-1.0.0
Status:	Initial canonical chain specification
Intended Audience:	OEMs, SDK implementers, certification counterparties, auditors
Date:	May 19, 2026

Abstract

This specification defines the certificate chain, signature schemes, attestation report format, freshness anchors, revocation mechanism, and Provenance Tier binding for telemetry that claims Provenance Tier $\tau \geq 3$. It is the operational complement to the Provenance Tier Taxonomy of Hardening Note v0.0.3 and the parametric predicate $P_T(y_k)$ of v0.0.4. TEEATTEST-1.0.0 is engineered so that the resulting attestations can be verified inside the GRSCHEMA-1.0.0 byte-canonical commitment without ambiguity across EVM, Substrate / Wasm, and Cairo / Starknet runtimes.

Contents

1. Scope and Status

TEEATTEST-1.0.0 is normative for any artifact claiming Provenance Tier $\tau \geq 3$ under S-0.0.4. RFC 2119 / RFC 8174 conventions apply.

This specification does *not* define a new proof system; cryptographic primitives are drawn from P-1.0.0 (Ristretto255 / Keccak-256), with the additional signature primitives enumerated in Section 3.

2. Architectural Model

2.1. Three-Layer Chain

BMS-TEE attestation in TEEATTEST-1.0.0 is a three-layer chain:

$$\underbrace{\text{StandardCo Root}}_{\text{Layer 0}} \rightarrow \underbrace{\text{OEM Root}}_{\text{Layer 1}} \rightarrow \underbrace{\text{Device Key}}_{\text{Layer 2}}$$

- **Layer 0 – StandardCo Root.** A long-lived offline root key controlled by IKKUNA as StandardCo. Used solely to certify Layer-1 OEM roots and to publish the Authoritative Revocation List.
- **Layer 1 – OEM Root.** An OEM-controlled signing key, certified by Layer 0. Used solely to certify Layer-2 device keys and publish per-OEM revocations.
- **Layer 2 – Device Key.** A per-asset key provisioned at manufacture inside the BMS-TEE silicon enclave. Used to sign telemetry observations y_t.

2.2. Tier Mapping

Tier	Required attestation
$\tau = 0$	Not in scope of this specification.
$\tau = 1$	Operator-key signature; not chained to Layer 0.
$\tau = 2$	Hardware-attested key at node boundary (TPM/HSM/TEE outside the asset); chain MAY terminate at a generic platform manufacturer root not certified by StandardCo.
$\tau = 3$	Full TEEATTEST-1.0.0 chain (Layer 0 $\rightarrow$ Layer 1 $\rightarrow$ Layer 2), Device Key resident in BMS-TEE silicon; ZK-continuity NOT required.
$\tau = 4$	Full TEEATTEST-1.0.0 chain (as $\tau = 3$) *plus* ZK-circuit verification of the thermodynamic continuity invariant per the Oracle-problem mitigation document.

2.3. Trust Boundary

The StandardCo Root MUST be kept offline (air-gapped) and used only at scheduled ceremonies. Layer-1 OEM roots MAY be online or HSM-hosted at the OEM's discretion, subject to Layer-0-published policy. Layer-2 device keys MUST never leave the BMS-TEE silicon enclave.

3. Cryptographic Suites

3.1. Signature Schemes

TEEATTEST-1.0.0 registers two signature suites. Each suite is identified by a `u16` *signature scheme identifier* (SSI).

SSI	Suite	Application
`0x0001`	Ed25519	Default for Layers 0–2 on platforms without HW-bound curve constraints.
`0x0002`	ECDSA P-256 (secp256r1)	For BMS silicon that ships HW-accelerated P-256 only.

Additional suites (e.g., post-quantum) MAY be registered by future TEEATTEST MINOR revisions. Suite removal requires a MAJOR bump.

3.2. Domain-Separated Signing

Every signature MUST be produced over the canonical byte sequence obtained by:

$$\sigma := \mathsf{Sign}_{sk}\big(\mathsf{utf8}(\mathit{label}) \,\|\, \mathsf{u32\_LE}(\mathrm{len}(\mathit{label})) \,\|\, \mathit{payload}\big),$$

with one of the following labels:

```
ONEDGE-SDK/v1/TEEATTEST/v1.0.0/L1Cert % Layer-0 -> Layer-1 certification
ONEDGE-SDK/v1/TEEATTEST/v1.0.0/L2Cert % Layer-1 -> Layer-2 certification
ONEDGE-SDK/v1/TEEATTEST/v1.0.0/Telem % Layer-2 telemetry signature
ONEDGE-SDK/v1/TEEATTEST/v1.0.0/Report % attestation report
ONEDGE-SDK/v1/TEEATTEST/v1.0.0/Revoke % revocation entry
```

These labels are non-substitutable: a signature produced under one label MUST NOT verify under any other.

3.3. Hashing

All hashing MUST use H_{P} from the prevailing P-version. For P-1.0.0, H_{P} = Keccak-256.

4. Certificate Format

4.1. Layer-1 Certificate (Layer-0 → Layer-1)

Field	Type	Semantics
`cert_version`	`u16`	`0x0100` for TEEATTEST-1.0.0
`cert_class`	`u16`	`0x0001` = Layer-1 (OEM root)
`issuer_root_id`	`bytes32`	Hash of StandardCo Layer-0 public key
`subject_oem_id`	`u32`	Registered OEM identifier (StandardCo registry)
`subject_oem_pk`	`bytes32`	OEM Layer-1 public key (compressed encoding for SSI suite)
`ssi_subject`	`u16`	Signature suite of subject key
`validity_h_from`	`u64`	Block-height start of validity
`validity_h_to`	`u64`	Block-height end of validity (zero = open-ended; see §7)
`policy_root`	`bytes32`	Merkle root of OEM-specific policy (allowed asset classes, ssi restrictions, key-rotation rules)
`signature_ssi`	`u16`	Signature suite used by issuer
`signature`	`bytes(*)`	Raw signature bytes, `u16`-LE length-prefixed (Ed25519 = 64 B; ECDSA P-256 = 64–72 B)

4.2. Layer-2 Certificate (Layer-1 → Layer-2)

Field	Type	Semantics
`cert_version`	`u16`	`0x0100`
`cert_class`	`u16`	`0x0002` = Layer-2 (device key)
`issuer_oem_id`	`u32`	As in the parent Layer-1 cert
`issuer_oem_pk`	`bytes32`	MUST match parent Layer-1 `subject_oem_pk`
`subject_device_pk`	`bytes32`	Device-key public component
`subject_asset_id`	`u128`	Asset to which this device key is bound
`asset_class_id`	`u32`	Registered asset-class identifier (BESS chemistry / form factor)
`ssi_subject`	`u16`	Signature suite of the device key
`validity_h_from`	`u64`	Block-height start of validity
`validity_h_to`	`u64`	Block-height end of validity (zero = open-ended)
`provenance_tier_max`	`u8`	Maximum τ this device key may attest (3 or 4)
`freshness_policy`	`u8`	Bitfield: bit 0 = require VDF anchor; bit 1 = require block-height anchor; others reserved = 0
`signature_ssi`	`u16`	Signature suite used by Layer-1 issuer
`signature`	`bytes(*)`	`u16`-LE length-prefixed

4.3. Canonical Serialization

Fields are serialized in the order shown, with no padding between fields. The *signing payload* for a certificate is the byte sequence consisting of all fields except `signature_ssi` and `signature`.

5. Telemetry Signature Format

A Tier-≥3 telemetry sample is a tuple

$$T := (asset\_id,\ channel\_id,\ sample\_h,\ value,\ freshness\_anchor,\ sig)$$

where:

Field	Type	Semantics
`asset_id`	`u128`	MUST match the binding in the device-key Layer-2 certificate
`channel_id`	`u32`	Per the GRSCHEMA-1.0.0 telemetry-channel registry
`sample_h`	`u64`	Sample block-height anchor
`value`	`u256`	Channel-typed value
`vdf_anchor`	`bytes32`	VDF output for the (sample_h - Δ_{VDF}) challenge, or zeros if not required by policy
`sig_ssi`	`u16`	Signature suite
`sig`	`bytes(*)`	`u16`-LE length-prefixed device-key signature

The *signing payload* is:

$$payload := \mathsf{u128\_LE}(asset\_id) \,\|\, \mathsf{u32\_LE}(channel\_id) \,\|\, \mathsf{u64\_LE}(sample\_h) \,\|\, \mathsf{u256\_LE}(value) \,\|\, vdf\_anchor.$$

The signature is produced under the label `ONEDGE-SDK/v1/TEEATTEST/v1.0.0/Telem`.

5.1. Freshness Anchors

A telemetry signature MUST include at least one freshness anchor, per the device key's `freshness_policy` bitfield:

- **Block-height anchor** (bit 1). `sample_h` MUST lie within $[h_{\text{verifier}} - \Delta_{\text{fresh}}, h_{\text{verifier}}]$ where Δ_{fresh} is the StandardCo-published freshness window (default: 256 blocks).
- **VDF anchor** (bit 0). `vdf_anchor` MUST equal the registered VDF output for the challenge committed at $sample\_h - \Delta_{\text{VDF}}$, with Δ_{VDF} the published VDF distance.

A telemetry observation lacking the policy-required anchor MUST be rejected with `ERR_TELEMETRY_STALE`.

6. Attestation Report

The attestation report is the artifact that the SDK consumes when computing $\tau(y_k)$ for each telemetry entry committed into a Golden Record.

6.1. Report Structure

Field	Type	Semantics
`report_version`	`u16`	`0x0100`
`asset_id`	`u128`	
`device_pk`	`bytes32`	Layer-2 device public key
`oem_pk`	`bytes32`	Layer-1 OEM public key
`l1_cert_hash`	`bytes32`	Keccak-256 of the canonical Layer-1 certificate
`l2_cert_hash`	`bytes32`	Keccak-256 of the canonical Layer-2 certificate
`revocation_root`	`bytes32`	Merkle root of the active revocation list at issuance
`issued_at_h`	`u64`	Block-height at which the report was produced
`tier_attested`	`u8`	3 or 4
`continuity_proof`	`bytes(*)`	`u16`-LE length-prefixed; required iff `tier_attested` = 4; empty otherwise

6.2. Validation Procedure (Verifier Side)

For each telemetry sample T within a Golden Record event, the verifier MUST execute the following procedure. Failure at any step MUST emit the named error code.

1. Lookup the active Layer-1 cert for `l1_cert_hash` in the StandardCo registry (`ERR_TEE_L1_UNREGISTERED`).
2. Verify the Layer-0 signature on the Layer-1 cert under its declared SSI (`ERR_TEE_L1_BAD_SIG`).
3. Verify that `issued_at_h` lies within the Layer-1 cert's validity window (`ERR_TEE_L1_EXPIRED`).
4. Lookup the Layer-2 cert by `l2_cert_hash` and verify the Layer-1 signature on it under its declared SSI (`ERR_TEE_L2_BAD_SIG`).
5. Verify `subject_asset_id` of the Layer-2 cert equals $T.asset\_id$ (`ERR_TEE_L2_ASSET_MISMATCH`).
6. Verify that `tier_attested` $\leq$ `provenance_tier_max` of the Layer-2 cert (`ERR_TEE_TIER_EXCEEDS_CERT`).
7. Verify the telemetry signature under the label `ONEDGE-SDK/v1/TEEATTEST/v1.0.0/Telem` using `subject_device_pk` (`ERR_TEE_TELEM_BAD_SIG`).
8. Verify freshness anchor(s) per the Layer-2 cert's `freshness_policy` (`ERR_TELEMETRY_STALE`).
9. Verify the device public key is NOT present in the active revocation list anchored by `revocation_root` (`ERR_TEE_KEY_REVOKED`).
10. If `tier_attested` = 4, verify the `continuity_proof` satisfies the Oracle-problem continuity invariant against the registered θ_a for the asset (`ERR_TEE_CONTINUITY_FAIL`).

The verifier's emitted Provenance Tier for T is then $\tau(T) :=$ `tier_attested` on success, or 2 if all steps 1–9 succeed but the asset's policy or device-key class is incompatible with tier 3 (`ERR_TEE_TIER_DOWNGRADED`). Across a vector y_k, the effective $\tau(y_k)$ is the minimum over required components per the v0.0.3 tier composition rule.

7. Revocation

7.1. Authoritative Revocation List (ARL)

StandardCo publishes the canonical `ARL.json` containing, for each revoked entity:

```
{
  "entity_type": "L1_CERT" | "L2_CERT" | "DEVICE_KEY" | "OEM_KEY",
  "entity_hash": "<keccak256 hex of canonical cert or pubkey>",
  "revoked_at_h": <u64 block height>,
  "reason_code": "KEY_COMPROMISE" | "POLICY_VIOLATION"
                 | "MANUFACTURER_RECALL" | "ROUTINE_ROTATION",
  "signature_ssi": <u16>,
  "signature": "<hex>"
}
```

Each entry MUST be signed by either Layer 0 (for any entity type) or Layer 1 (for its own subordinate Layer 2 entries) under the label `ONEDGE-SDK/v1/TEEATTEST/v1.0.0/Revoke`.

7.2. Revocation Root

The StandardCo-published `revocation_root` is the Keccak-256 Merkle root over the ARL leaves, sorted ascending by `entity_hash`. Each leaf is:

$$leaf := H_{\mathsf{P}}\big(\mathsf{utf8}(\text{“ONEDGE-SDK/v1/TEEATTEST/v1.0.0/Revoke”}) \,\|\, \mathsf{u32\_LE}(\mathrm{len}_{\mathsf{label}}) \,\|\, canonical\_entry\big).$$

Internal nodes use the same hash composition rule as GRSCHEMA-1.0.0 §4.

7.3. Non-Retroactivity

A revocation MUST NOT retroactively invalidate Golden Record records committed prior to `revoked_at_h`. Records committed at or after `revoked_at_h` that reference the revoked entity MUST be rejected.

8. Key-Provisioning Requirements (OEM)

OEMs claiming TEEATTEST-1.0.0 conformance MUST satisfy:

Requirement 1 (Silicon-bound key generation)**.** The Layer-2 device key MUST be generated inside the BMS-TEE silicon enclave during manufacture or first-boot ceremony, with the private component never crossing the silicon boundary.

Requirement 2 (Tamper-resistant storage)**.** Layer-2 private keys MUST be stored in tamper-resistant memory that satisfies the platform's published security claim (e.g., FIPS 140-3 Level 3 for the silicon enclave, or an equivalent published claim).

Requirement 3 (Asset binding)**.** The Layer-2 certificate MUST be issued by Layer-1 within Δ_{prov} blocks of device-key generation (default: 4096 blocks). StandardCo MAY tighten this window per OEM via the Layer-1 cert's `policy_root`.

Requirement 4 (No key replication)**.** The same Layer-2 public key MUST NOT appear in more than one Layer-2 certificate. Conformant Layer-1 issuers MUST refuse duplicate subjects.

Requirement 5 (Key rotation)**.** Layer-1 OEM keys SHOULD be rotated at least every 4 years. Layer-0 StandardCo root key SHOULD be rotated at least every 7 years. Rotation MUST be performed under a publicly announced ceremony with an audit trail satisfying the StandardCo charter (when published).

9. Reason Codes

The following reason codes are introduced by TEEATTEST-1.0.0, complementing those of I-1.0 and GRSCHEMA-1.0.0:

Code	Semantics
`ERR_TEE_L1_UNREGISTERED`	Layer-1 cert not in StandardCo registry.
`ERR_TEE_L1_BAD_SIG`	Layer-0 signature on Layer-1 cert failed verification.
`ERR_TEE_L1_EXPIRED`	`issued_at_h` outside Layer-1 validity window.
`ERR_TEE_L2_BAD_SIG`	Layer-1 signature on Layer-2 cert failed verification.
`ERR_TEE_L2_ASSET_MISMATCH`	Layer-2 cert subject asset does not match telemetry asset.
`ERR_TEE_TIER_EXCEEDS_CERT`	`tier_attested` > `provenance_tier_max`.
`ERR_TEE_TIER_DOWNGRADED`	Policy / asset class incompatible with declared tier.
`ERR_TEE_TELEM_BAD_SIG`	Device-key signature on telemetry failed verification.
`ERR_TEE_KEY_REVOKED`	Device key on active revocation list.
`ERR_TEE_CONTINUITY_FAIL`	Tier-4 continuity proof failed verification.
`ERR_TEE_FRESHNESS_VDF`	VDF anchor mismatch.

10. Binding to GRSCHEMA-1.0.0

A telemetry entry in y_k carries `tier` $\in \{0, 1, 2, 3, 4\}$ and `attestation_root` per GRSCHEMA-1.0.0 §3.4. Under TEEATTEST-1.0.0, for `tier` ≥ 3 the `attestation_root` MUST equal the Keccak-256 of the canonical attestation report (Section 6), hashed under the label `ONEDGE-SDK/v1/TEEATTEST/v1.0.0/Report`.

StandardCo publishes a registry mapping attestation-report hashes to the underlying reports. Verifiers MAY fetch the report on-demand for full validation; the on-chain commitment retains the hash only.

11. Threat Model

TEEATTEST-1.0.0 mitigates, in particular:

- **Operator-side SCADA spoofing:** prevented by requiring silicon-rooted Layer-2 signatures for $\tau \geq 3$ statements; SCADA becomes a transport only.
- **Key replication across assets:** prevented by Requirement R4 and Layer-1 issuance discipline.
- **Stolen device key:** mitigated by ARL and per-asset binding (a stolen key is bound to a specific `asset_id` and rapidly revocable).
- **Replay across time:** mitigated by mandatory freshness anchors (block-height or VDF).

- **Cross-OEM impersonation:** prevented by per-OEM Layer-1 issuance and the Layer-0 / Layer-1 / Layer-2 chain.
- **Sensor drift past tolerance:** indirectly addressed; drift is detected by the Tier-4 continuity check (Oracle-problem mitigation) and reported by the verifier as `ERR_TEE_CONTINUITY_FAIL`.

The specification does *not* mitigate physical-bypass attacks at silicon level; such attacks remain a residual risk shared with all hardware-rooted attestation systems.

12. Conformance

A conformance implementation MUST:

1. Reproduce all certificate canonical byte sequences and signature payloads exactly as specified.
2. Accept all valid certificate chains and reject all invalid chains per Section 4.
3. Reject any telemetry sample whose verification path produces any of the reason codes in Section 9.
4. Reproduce the conformance vectors at `conformance-vectors/teeattest-1.0.0/` (to be generated in a follow-up release).
5. Bind Golden Record telemetry entries' `attestation_root` per the rule in Section 9.

Disclaimer

This document is a normative attestation-chain specification prepared by IKKUNA SpA. It does not constitute legal, financial, investment, regulatory, engineering, tax, or professional advice. ONEDGE ENERGY remains a proposed open standard and candidate specification in pre-TRL-7 validation status.