STEA-M v0.1

Spatio-Temporal External Attestation Mechanism

Public Prior Art

January 17, 2026

Abstract

STEA-M is a minimal, device-anchored mechanism for producing post-verifiable spatio-temporal attestations. The system enables verification that a physical device was present at a compatible geographic location during a constrained time window and had simultaneous access to multiple independent external reference services. STEA-M does not attest content truth, human identity, or continuous activity. It is published as open prior art.

1 Design Goals

STEA-M is designed to satisfy the following constraints:

- Post-verifiability
- Minimalism
- Device anchoring (non-personal)
- Fail-secure operation
- Privacy preservation

2 Definitions

2.1 STEA-D (Device)

A STEA-D is a physical device capable of:

- secure key storage
- external time acquisition
- external randomness acquisition
- GNSS positioning
- cryptographic hashing

2.2 Attestation Window

A bounded time interval $[t_0, t_1]$ during which all external inputs MUST be acquired.

3 External Reference Inputs

3.1 Time Anchors

At least two independent time sources MUST be used, selected from:

- GNSS system time
- authenticated network time services
- institutional time beacons

Attestation MUST be aborted if the time skew exceeds a predefined tolerance $\Delta t_{\max}$.

3.2 Randomness Anchor

STEA-M requires external entropy with the following properties:

- unpredictability during the attestation window
- reconstructability a posteriori
- public consistency for the same window

Internal-only randomness MUST NOT be used.

3.3 GNSS Location Anchor

GNSS positioning MUST support multi-constellation operation (e.g., GPS, Galileo, GLONASS, BeiDou).

Recorded data MUST include:

- latitude, longitude (altitude optional)
- timestamp
- constellation identifiers
- satellite identifiers

4 Device Identity

4.1 Device Identifier

Each device has a deterministic identifier:

$$ID_{dev} = HASH(Manufacturer\_ID \parallel Serial \parallel HW\_Fingerprint \parallel PubKey)$$

The identifier is non-reversible and contains no personal data.

4.2 Manufacturer Registry

A public, append-only registry contains:

- Manufacturer identifier
- root public keys
- status information

The registry is informational and non-authoritative.

5 Attestation Generation

5.1 Trigger

Attestation MUST be initiated by an explicit physical user action.

5.2 Acquisition Phase

During the attestation window, the device MUST acquire:

1. external randomness sequence R_{ext}
2. reconciled time anchor T_{anchor}
3. GNSS fix G

Failure of any step aborts attestation.

5.3 Commitment Construction

The commitment is computed as:

$$C = HASH(ID_{dev} \parallel R_{ext} \parallel T_{anchor} \parallel G \parallel Version)$$

Canonical encoding and ordering MUST be used.

5.4 Output

The device outputs:

- a numeric digest and/or
- a QR-encoded representation of C

6 Verification

Verification consists of:

1. recomputing external randomness for the window
2. validating time consistency
3. validating GNSS plausibility
4. recomputing the commitment
5. comparing against the provided value

Verification does not require access to the original device.

7 Revocation and Ownership

7.1 Revocation

Devices MAY be marked as:

- ACTIVE
- REVOKED
- STOLEN
- DECOMMISSIONED

Revocation affects future trust but does not invalidate past attestations.

7.2 Ownership Change

Ownership change is handled via key rotation. The device identifier remains unchanged.

8 Threat Model

8.1 Mitigated Attacks

- replay
- backdating and forward-dating
- offline fabrication
- AI-generated context forgery

8.2 Out-of-Scope Attacks

- content falsification
- staged real-world events
- invasive hardware attacks
- state-level GNSS spoofing

9 Fail-Secure Behavior

STEA-M MUST:

- produce no output on failure
- avoid degraded or fallback modes
- never simulate missing inputs

10 Non-Goals

STEA-M does not provide:

- proof of truth
- proof of human identity
- media authenticity
- continuous tracking
- surveillance functionality

11 Ethical Position

STEA-M is designed to enable verification without surveillance, accountability without identity exposure, and openness without central control.

12 Declaration of Intent

STEA-M is published as open prior art. Any party may implement, modify, or extend the method without restriction.