

EVSE Compliance Lifecycle Data Standard

Concept overview and draft minimum data element set · August 2026

1. Purpose

Define a uniform, machine-readable structure for the facts that jurisdictions, operators, and registered service agencies already exchange about commercial EVSE — so the same fact is expressed the same way everywhere, and every event in a device’s service life appends to one continuous record. The standard specifies **data, not policy**: each jurisdiction retains full authority over what it requires, when, and from whom. The standard only ensures that whatever is required can be filed, read, and audited in common form.

2. Design principles

Device-keyed. The record is anchored to the device serial number and NTEP Certificate of Conformance — the two identifiers that already exist in every jurisdiction’s process.

Event-based and append-only. Each lifecycle stage emits a typed event appended to the record. Prior events are never modified; corrections are new events referencing the record they correct. The record is tamper-evident by construction — the audit-trail discipline this Sector has long applied to metrologically significant software, extended to the compliance record itself. Means of assuring integrity are left to the work group.

Role-typed actors. Every event names its actor as operator, registered service agency (with registration number), jurisdiction, or system — so who did what is a queryable field, not prose.

Per-device violation scope. A violation and its correction are keyed to the specific device or port at issue. A correction amends the affected record only; accepted filings for unaffected devices are never reopened.

Record-attached correspondence. Communications concerning a device are part of its record — appended, attributed, and retrievable with it — so coordination among jurisdiction, service agency, and operator accrues to the record rather than to inboxes.

Transport-agnostic. The schema defines content, not carriage. A conforming record can move by portal upload, email attachment, or API — jurisdictions adopt at their own pace without stranding anyone.

3. Lifecycle model

EVSE COMPLIANCE LIFECYCLE — one continuous record per device (serial number + CoC)

Every stage emits a standardized, machine-readable event appended to the same device record.

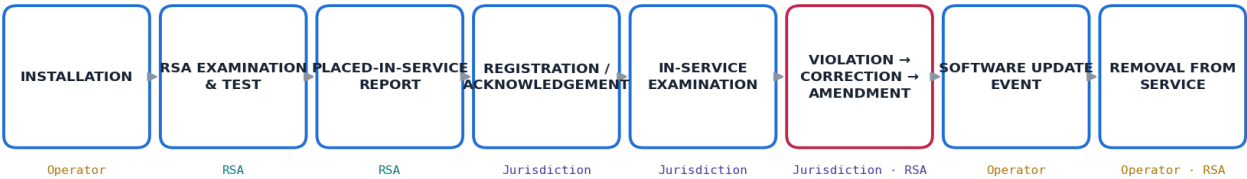


Figure B-1. One continuous record per device. Actors shown beneath each stage.

4. Draft minimum data element set

Every event shares a common envelope; each event type adds its own elements. The set below is a starting point for work-group refinement, not a finished specification.

Record / event type	Minimum data elements
Common envelope (all events)	Record ID · device serial number · CoC number · event type · timestamp (UTC) · actor role and identifier (RSA registration number where applicable) · jurisdiction code
Device identity block	Manufacturer · model · serial number · CoC number · connector/port inventory · metrologically significant software version · seal/audit-trail category and status
Installation	Site address and geocode · operator of record (name, address, contact) · site host distinction · commissioning date
Placed-in-service report	Examining RSA · examination date · per-port scope · test standard used and traceability · as-found / as-left results · result disposition · filing timestamp
Temporary authorization (TUP)	Permit ID · issuing jurisdiction · issue date · expiration / upgrade-due date · conditions (e.g., obtain CoC, install certified software build) · status effect on expiry
Examination request / scheduling	Requesting party (jurisdiction) · request type (on-site presence · witness test) · device or site scope · proposed and confirmed dates · responding party and response · reference to the resulting examination event
Examination (RSA or jurisdiction)	Examination type · checklist items evaluated with pass/fail per item · accuracy results per port · examiner identity · witnessed-by attribute (witnessing jurisdiction and examiner, where a jurisdiction observes a service agency or manufacturer test)
Violation	Citation ID · requirement cited (Handbook 44 / jurisdiction code reference) · scope (device / port) · status effect (removed from service or not) · response window
Correction / amendment	Amendment ID · referenced citation · corrective action · re-examination results · scope limited to affected device or port
Software update	Prior and new version identifiers · metrological significance flag · updated identity block export
Removal from service	Reason · disposition · final record close-out

5. Relationship to existing NCWM / NIST instruments

The standard sits inside the existing architecture rather than beside it. **Handbook 44 § 3.40** and **EPO 30** define what is examined; the standard defines how the outcome is recorded and exchanged. **Publication 14** is the natural home for the device-side requirement — that the identity block and metrologically significant software version be exportable in the standardized format (proposed amendment language appears in the agenda item). **Handbook 130** uniform-regulation work on registration remains complementary: a model regulation says what must be filed; this standard ensures every filing is readable everywhere.

6. The registry: a single source of truth

Once filings share one structure, a national registry becomes an aggregation, not an invention: one record per device, keyed to serial number and CoC, receiving standardized events and giving each jurisdiction a continuous, auditable view of every device in its territory. Conceptually this extends the NTEP CoC database — the single source of truth for type approval — forward into field compliance. Jurisdictions remain sovereign over their data and their requirements; the registry gives them, for the first time, a common place to look. One record supports three role-scoped views — a jurisdiction console, a service agency workbench, and an operator dashboard — so a device's entire lifecycle history is a single query for every authorized party, not a correspondence chain.

A working implementation of this record structure exists today and is the source of the rendered figures in Attachment C — demonstrating that the model is buildable with current technology. The purpose of this item is to ensure the structure itself becomes a national, vendor-neutral standard rather than a set of incompatible private ones.