

Audit - Format, Remote, Local, Cadence (S9-S12)

§9 — Audit package format & storage

Each signed invoice yields an audit package containing the invoice `{ request, result }`. The package is encrypted as follows:

- **Payload** — encrypted with **AES-256 (CBC, PKCS7 padding)** using a one-time key and IV.
- **Key transport** — the one-time AES key and IV are **RSA-encrypted with the TaxCore public key**.
- **Package** — `{ key, iv, payload }`, identical in form for both remote and local audit.

Packages are written to non-volatile storage before the POS response returns, and are **never overwritten or erased without a proof-of-audit**: a package is retained until it is verified (accepted) or cleared by a valid POA. Applying a POA to the SE (End Audit) resets the held amount, after which the corresponding packages may be cleared. Packages are keyed by SE UID, so switching cards does not interrupt an in-flight audit.

§10 — Remote audit protocol

When connectivity is available, a background auditor submits audit packages to TaxCore continuously and flushes any previously unsent packages. The protocol uses the specified endpoints:

Operation	Purpose
Submit audit	Upload encrypted audit packages.
Audit proof	Receive the proof-of-audit for application to the SE.
Online status	Periodic heartbeat while a valid token is held.
Commands	Retrieve and acknowledge TaxCore commands (§4).

`auditRequired` is surfaced in Get Status when the SE nears or reaches its limit. Submission continues automatically whenever data and internet are available; this has been demonstrated live clearing a full SE ($\approx 12\text{M}$) to zero.

§11 — Local audit (removable media)

For prolonged offline operation, audit data is carried on USB/SD media using the same package format as remote audit.

Export

- A sub-folder named by the SE UID is created on the media if absent: `{root}\{UID}\`.
- The audit request produced by Start Audit is written as `{UID}.arp`.
- Each audit package is written as an individual JSON file in the specified `{UID}-{UID}-{n}.json` convention.
- Started / in-progress / completed status is shown in the Local Audit panel.

Import (proof-of-audit)

- The commands file `{UID}.commands` is read from the media and executed.
- The proof-of-audit is applied to the SE via End Audit.
- Results are written back as `{UID}.results`.

§12 — Proof-of-Audit cadence

A shared cadence guard governs both the manual and background audit paths so that only one Audit Start is outstanding at a time. This prevents a second Start from invalidating an earlier, still-pending proof.

- **Minimum between Starts:** 10 minutes (well above the 5-minute minimum).
- **Normal cadence:** 30 minutes; tightened as the SE approaches its limit.
- A proof-of-audit is applied to the SE as soon as it is received; memory is cleared only after the POA resets the held amount.

Revision #1

Created 2026-08-13 08:42:43 UTC by Shanil Verma

Updated 2026-08-13 08:42:43 UTC by Shanil Verma