

Architecture & Secure Element (S1-S2)

§1 — System architecture & components

XPOS ESDC is an application-based E-SDC for Windows 10/11 (x64). It is a single self-contained package that runs a background fiscal service and an operator UI in one process, so the UI and the POS-facing service share one Secure Element access lock, PIN cache and data store.

Component	Role
Operator UI (tray application)	Status, built-in POS, reports, audit controls, About (Manufacturer / Serial / Software version / Model / SE applet version).
POS-to-SDC service (localhost:8888)	Receives invoice requests from the built-in or a third-party POS (v3, legacy V2 supported).
Secure Element access layer	PC/SC (APDU) to the SE applet; PKCS#11 to the PKI applet. Serialised behind a single card lock.
Audit & command services	Background services for remote audit, proof-of-audit cadence, online-status and command processing.
Local store	Embedded database for invoice records and encrypted audit packages; plain-text log folder.
Token helper	Small native helper performing the mutual-TLS token request over the card key (see §3).

Program files install under Program Files (read-only at runtime); working data (records, logs, settings) is kept in the per-user application-data folder. All configuration originates from the Secure Element at runtime.

§2 — Secure Element interface

All fiscal signing and all fiscal counters are performed and held on the Secure Element (SE); XPOS ESDC never computes or alters fiscal signatures. The SE is reached through an external USB PC/SC reader using ISO 7816 APDUs.

- **PIN verification** — a Verify APDU unlocks signing. The PIN is supplied by the operator and held only in memory (§17).
- **Sign** — the invoice request (date/time, amount, counters, tax data) is sent to the SE, which returns the signature, encrypted internal data and updated counters.
- **Amount / limit** — the SE accumulates a signed amount and reports when an audit is required; XPOS ESDC reads this for status and audit triggering.
- **Start / End Audit** — Start Audit produces the audit request (ARP); End Audit applies a proof-of-audit and resets the held amount.

Signing does not require connectivity; an invoice can be fully fiscalised offline.

Revision #1

Created 2026-08-13 08:42:41 UTC by Shanil Verma

Updated 2026-08-13 08:42:41 UTC by Shanil Verma