

Digital Signatures & Verification (S8)

§8 — Digital signature & verification URL

Every invoice type — Normal, Advance, Copy, Training, Proforma — is signed on the SE and produces a unique verification URL encoded into the receipt QR code. The URL payload is assembled to the FRCS specification and comprises:

- Format version;
- Secure Element UID and requesting-signer identifiers;
- Invoice and total counters;
- Total amount and timestamp;
- Encrypted internal data;
- The SE signature; and
- An integrity digest (MD5) over the payload.

The signature allows any party to verify the invoice's integrity and authenticity via the verification URL / FRCS portal. The exact byte layout and QR encoding conform to the FRCS E-SDC specification and are validated by the SDC Analyzer.

Signing mechanism

The invoice is not signed by XPOS ESDC itself — it is signed by the Secure Element. XPOS ESDC builds the signing payload (including the trusted SDC clock's timestamp) and hands it to the SE over PKCS#11; the SE's private key never leaves the card, and the signature it returns is what gets embedded in the verification URL. This is what makes the signature genuine cryptographic authenticity rather than a simple checksum: only the specific Secure Element holding that private key could have produced a signature that validates.

Because the FRCS token endpoint requires the client certificate via TLS renegotiation, which managed .NET TLS stacks cannot perform, this handshake and the signing call are carried out by a small bundled native helper (using the card key over PKCS#11/OpenSC) rather than XPOS ESDC's own managed code directly.

Verification

Anyone with the verification URL — scanned from the receipt QR code or read from the invoice — can independently confirm the invoice was genuinely signed by that Secure Element and has not been altered since, without needing access to XPOS ESDC, the Secure Element, or Defy Technologies' own systems.

Revision #2

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

Updated 2026-09-30 09:47:10 UTC by Shanil Verma