ENGINEERING SPECIFICATION

version 9.0

INTERNET IDENTITY CARD ™

Provenance, engineering innovations & standards compliance

Issuer	Https Card — Internet Identity Card Ltd
Company Registration	UK Companies House No. 09168431
Trademark	UK IPO UK00003166480 (2016) · INPI FR 4071419
US Copyright	TX 8-508-373 (2014/2017)
Office	124 City Road, London EC1V 2NX, United Kingdom
Disclosures	TDCommons #10079 · #10167 · #10394 (CC BY 4.0)

This document supersedes the v8.4.1 edition. It documents the hybrid post-quantum posture introduced in IIC v9.0: signatures combine the classical ECDSA P-256 algorithm with the post-quantum ML-DSA-65 (FIPS 204) algorithm, following ANSSI transition guidance.

1. Provenance & priority

The Internet Identity Card project has been developed continuously since 2013 by Https Card — Internet Identity Card Ltd (UK Companies House No. 09168431). Priority and prior-art positions are documented through independent, verifiable channels:

- **US Copyright** TX 8-508-373 — source created 2014, registered 2017 (publicrecords.copyright.gov, record voyager_29764072).
- **Trademarks** — UK IPO UK00003166480 (2016); INPI FR 4071419.
- **Defensive publications** — TDCommons #10079, #10167, #10394 (CC BY 4.0).
- **Blockchain anchors** — Bitcoin anchor of 13 May 2019; cumulative Bitcoin + Ethereum anchors #2–#4 (2026) over the complete package; per-document anchors where applicable.
- **Regulatory registrations** — ICO ZA457585 (UK), CNIL 1726245 (France), D&B DUNS 220301971.

The work is positioned as documented prior art in the self-sovereign, offline-first identity space (situated against TDCommons #10167), not as a claim of exclusive novel invention.

2. Core engineering innovations

2.1 Single-file, zero-dependency architecture

The complete application — cryptography, UI, verification — lives in one HTML file. No external script, no CDN, no server round-trip. This constraint drives most engineering decisions: crypto primitives are embedded, styles inlined, and the exported card carries its own verification engine.

2.2 Offline self-verification

A DOM-snapshot integrity mechanism: the document hashes its own canonical serialization (captured before script mutations, with dynamic elements normalized) and compares it against an embedded digest. Sealing at generation time uses a hidden iframe (srcdoc) to compute the final hash. Fail-closed lockdown on mismatch. Verified functional in airplane mode.

2.3 Hybrid post-quantum signing (new in v9.0)

v9.0 integrates a crypto-agile hybrid suite: ECDSA P-256 + ML-DSA-65 (FIPS 204), implemented with @noble/post-quantum (pure JavaScript, no WASM). Both the card identity and document-signing receipts (v3.0) carry dual signatures. Design constraints honored:

- **Additive, never blocking** — PQC signing is wrapped so card creation and classical signing continue even if the module fails.
- **Backward compatible** — ECDSA is preserved; v2.0 receipts remain verifiable.
- **CSP-safe embedding** — the exported card receives its verification engine as a base64 payload activated via an inline script element created with textContent (no eval, no WASM).
- **Deterministic modular build** — source modules are bundled reproducibly (identical sources yield an identical file SHA-256), a prerequisite for meaningful blockchain anchoring.

2.4 Multi-zone canonical neutralization

A self-serialized document simultaneously carries heterogeneous-size hybrid signatures, a self-referential integrity digest, and a post-signing anchor reference, resolved via a fixed neutralization order with length-preserving placeholders. Documented as a defensive publication (see the IIC Defensive Publication on canonical multi-zone neutralization).

3. Immutability & regulatory considerations

Once exported, a card is immutable by construction: any modification breaks the SHA-256 self-check. The system stores no personal data server-side (there is no server); GDPR obligations rest with the holder as the data controller of their own file. Registrations with the ICO (ZA457585) and CNIL (1726245) document the company's compliance posture.

4. Standards compliance

Standard	Use in IIC v9.0
AES-256-GCM (NIST SP 800-38D)	Identity encryption at rest
Argon2id (RFC 9106)	Key derivation — 96 MiB, t=4, p=4
SHA-256 (FIPS 180-4)	Integrity, signed-core digests, anchoring
ECDSA P-256 (FIPS 186-5)	Classical signature component
ML-DSA-65 (FIPS 204)	Post-quantum signature component
W3C CSP Level 3	Hardened generator and card policies

Conformance note. “FIPS 204-conformant” describes algorithmic conformance in code. It is distinct from FIPS 140 CMVP module validation and from ANSSI qualification (CESTI evaluation), which are formal third-party processes.

5. Change history (engineering)

- **v8.3** → **v8.4** — offline self-verification (DOM snapshot), airplane-mode fix.
- **v8.4** → **v8.4.1** — backup KDF upgraded PBKDF2 → Argon2id (96 MiB, t=4, p=4, random per-backup salt); UI/code KDF mismatch corrected.
- **v8.4.1** → **v9.0** — hybrid post-quantum signing (identity + documents), embedded verification engine in exported cards, deterministic modular build, receipts v3.0.

6. Issuer information

Https Card — Internet Identity Card Ltd · UK Companies House No. 09168431 · 124 City Road, London EC1V 2NX, United Kingdom. Trademarks UK00003166480, FR 4071419. US Copyright TX 8-508-373. TDCommons #10079 · #10167 · #10394. © 2013–2026.