THREAT MODEL

version 9.0

INTERNET IDENTITY CARD ™

Security analysis, trust assumptions & residual risks

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. Scope & objectives

This document describes the threat model of the Internet Identity Card (IIC) v9.0: the assets it protects, the adversaries it defends against, and the residual risks it does not. It supersedes the v8.4.1 threat model. The central change in v9.0 is the introduction of a **hybrid post-quantum signature**: where signing is enabled, a card and the documents it signs carry both a classical ECDSA P-256 signature and a post-quantum ML-DSA-65 (FIPS 204) signature, verified together.

A threat model is not a security guarantee. It states what the system is designed to do under stated assumptions; the conditions under which those protections do not apply are documented in Section 8.

2. System overview

The IIC is a single self-contained HTML file. Identity data is encrypted at rest with AES-256-GCM under an Argon2id-derived key. The file verifies its own integrity offline via an embedded SHA-256 of its own serialization. Where authorship must be provable, the issuer signs the card identity and any signed documents with the hybrid suite. Blockchain anchoring (Bitcoin and Ethereum) provides authority-free proof of existence at a date. No server, PKI, or certificate authority is involved at any point; verification runs in a vanilla browser, offline.

3. Trust assumptions

The security properties in Sections 6 and 7 hold only while these assumptions are true:

- The device and browser executing the file are not compromised.
- The passphrase is chosen well and kept secret.
- Public keys used to verify a card are obtained from a trusted channel; the file proves *what* was signed, not *who* the signer is.
- For post-deprecation verification, the verifier can consult a blockchain header chain to confirm an anchor timestamp.

4. Assets under protection

Asset	Protection
Identity data at rest	AES-256-GCM, Argon2id-derived key (96 MiB, t=4, p=4)
File integrity	Embedded SHA-256 self-check, fail-closed lockdown, offline
Authorship	Hybrid ECDSA P-256 + ML-DSA-65 signature over the signed core
Proof of existence at a date	Bitcoin + Ethereum timestamp anchors

5. Adversaries & capabilities

- **A1 — Network adversary.** Sees or alters data in transit. Defeated by offline operation and AES-256-GCM.
- **A2 — Storage adversary.** Obtains the file at rest. Faces AES-256-GCM + Argon2id.
- **A3 — Forger.** Attempts to alter a card or forge a signature. Faces SHA-256 self-integrity and the hybrid signature (both components required).
- **A4 — Quantum adversary (future).** A large fault-tolerant quantum computer able to run Shor's algorithm against ECDSA P-256. **New in v9.0:** this adversary is now explicitly addressed — see Sections 6 and 8.

6. STRIDE analysis

Mapping the six STRIDE categories onto the IIC v9.0 architecture.

Category	Applied to IIC v9.0	Disposition
Spoofing	Hybrid ECDSA P-256 + ML-DSA-65 signing binds a card to an issuer key. A valid signature requires *both* private keys, so forging one component is insufficient.	**MITIGATED**
Tampering	SHA-256 page self-integrity with fail-closed lockdown detects any byte change outside the hash zone, verifiable fully offline.	**PROTECTED**
Repudiation	No central log; blockchain timestamping (BTC/ETH) provides external, tamper-evident proof of existence at a date.	**MITIGATED**
Information disclosure	AES-256-GCM with Argon2id-derived keys protects identity at rest and in transit.	**PROTECTED**
Denial of service	A single offline file has no service to deny; loss of file or passphrase means loss of access, by design.	**PROTECTED**
Elevation of privilege	Strict CSP and Permissions-Policy disable camera, microphone, geolocation, payment and USB in the exported card.	**PROTECTED**

7. Concrete attack scenarios

- **Byte-level tamper.** Any change outside the hash zone breaks the SHA-256 self-check → fail-closed lockdown. Detected offline.
- **Signature forgery (classical).** Forging ECDSA alone fails: the ML-DSA-65 component must also verify. An attacker without the post-quantum private key cannot produce a valid hybrid signature.
- **Harvest-now, decrypt-later (confidentiality).** An adversary storing an encrypted card today cannot decrypt it with a future quantum computer: AES-256 retains ~128-bit security under Grover's algorithm, which remains computationally infeasible.
- **Harvest-now, forge-later (retrospective forgery).** An adversary storing a signed card today, intending to break ECDSA with a future quantum computer, cannot forge authorship: ML-DSA-65 remains secure, and the blockchain anchor proves the card existed before ECDSA deprecation.
- **Post-deprecation forgery.** After ECDSA is deprecated, a forged card carrying only a quantum-broken ECDSA signature fails ML-DSA-65 verification and lacks a valid pre-deprecation anchor.

8. Residual risks & out of scope

A credible threat model names what it does not defend against. The following remain out of scope for IIC v9.0:

- **Compromised endpoint.** A malicious browser or OS can subvert any in-page cryptography.
- **Key custody.** The system proves what was signed, not that the signer's key belongs to a particular real-world identity; that binding is external.
- **Offline revocation.** A frozen offline file cannot receive a revocation signal without an information channel; short-lived credentials or pre-downloaded status lists remain the realistic approaches.

Quantum adversaries — updated posture. AES-256 retains ~128-bit strength under Grover. Unlike v8.4.1, ECDSA P-256 is *no longer the sole authorship mechanism*: v9.0 adds ML-DSA-65 (FIPS 204), a post-quantum

signature, in a hybrid construction. A large fault-tolerant quantum computer able to break ECDSA does *not* break the card's authorship, because the ML-DSA-65 component remains secure and the blockchain anchor evidences pre-deprecation existence. This follows ANSSI's stated preference for hybrid (classical + post-quantum) constructions during the transition period. Note: hybrid PQC-readiness in code is distinct from a formal ANSSI qualification, which requires evaluation by an approved CESTI laboratory.

9. Operational recommendations

- Enable hybrid signing when authorship needs to be provable.
- Anchor the card or its package to Bitcoin/Ethereum to obtain proof of existence at a date.
- Retain a blockchain header chain (or access to one) for long-term post-deprecation verification.
- Treat the passphrase as the root secret; its loss is unrecoverable by design.

10. Disclaimer

This threat model is provided for informational purposes only. It describes intended security properties under the trust assumptions of Section 3. Where those assumptions do not hold, the protections described may not apply. “PQC-ready” denotes conformance to the ML-DSA (FIPS 204) standard in code; it does not constitute a FIPS 140 CMVP validation or an ANSSI qualification, both of which require formal third-party evaluation.