ENGINEERING SPECIFICATION

version 8.4.1

INTERNET IDENTITY CARD ™

Innovations, provenance and regulatory framework of IIC v8.4.1

Issuer	Https Card — Internet Identity Card Ltd
Company Registration	UK Companies House No. 09168431
Trademark	UK IPO UK00003166480 (2016)
Office	124 City Road, London EC1V 2NX, United Kingdom
File size	~336 KB (single self-contained HTML file)

Important notice

Legal & regulatory disclaimer

NATURE OF THE PRODUCT

Internet Identity Card ™ is a private software-based identity and verification platform developed by Https Card — Internet Identity Card Ltd. It is not a government-issued identity document and is not an officially recognised electronic identification scheme unless specifically recognised by applicable law in a given jurisdiction.

TRADEMARK NOTICE

Internet Identity Card — Prove and Protect Your Online Identity ™ is a trademark of Https Card — Internet Identity Card Ltd, registered with the UK Intellectual Property Office (UK00003166480).

REGULATORY DISCLAIMER

References in this document to electronic signatures, eIDAS, international organisations, cybersecurity initiatives, or regulatory frameworks are provided for informational purposes only. Such references do not constitute certification, accreditation, endorsement, or legal recognition by any of the entities or frameworks mentioned. The cryptographic signatures produced by IIC are technical artifacts and are not inherently legally binding unless recognised under applicable law.

SECURITY DISCLAIMER

No software system can be guaranteed to be completely secure. The cryptographic properties described in this document are based on established algorithmic assumptions (NIST FIPS 197, SP 800-132, FIPS 186-4, RFC 6238) and are designed to substantially reduce — not eliminate — the risk of unauthorised access, modification, or impersonation. Users remain responsible for the operational security of their own devices, authentication factors, and exported card files.

NO ENDORSEMENT

Internet Identity Card ™ is an independent project. Participation in international discussions, public consultations, or working groups does not imply endorsement or adoption by the institutions mentioned.

© 2013–2026 Https Card — Internet Identity Card Ltd
UK Co. 09168431 · Trademark UK00003166480 · 124 City Road, London EC1V 2NX, United Kingdom

1. Provenance & priority

The Internet Identity Card project is owned and operated by Https Card — Internet Identity Card Ltd, a UK company incorporated in 2014 (company number 09168431) and holder of the UK trademark UK00003166480 ("INTERNET IDENTITY CARD"), filed on 25 May 2016. The inventor's first public work on the Internet Identity Card concept dates from 2013 under the domain httpscard.com, with the domain internetidentitycard.com registered as a continuation on 5 January 2014. The trademark and the underlying engineering work predate by several years any comparable commercial "digital identity card" product.

1.1 Documented timeline

2013	First public work on Internet Identity Card by the inventor under the domain httpscard.com.
5 January 2014	Registration of internetidentitycard.com (continuation of httpscard.com).
2014	Incorporation of Https Card — Internet Identity Card Ltd (UK 09168431).
25 May 2016	Filing of UK trademark UK00003166480 ("INTERNET IDENTITY CARD").
May 2019	Public deployment of the v6 single-file generator on IPFS with Bitcoin blockchain timestamping via OriginStamp.
2023–2025	Iterative releases v7 to v8.3 (dual-domain key derivation, TOTP obfuscation, IIFE module isolation).
12 May 2026	TDCommons defensive publication #10079 — TOTP-derived symmetric keys for offline issuer-mediated access control.
17 May 2026	v8.4 release: Argon2id migration, SHA-256 page integrity, dual-passphrase architecture.
May 2026	TDCommons defensive publication #10167 — self-verifying single-file documents with dual-passphrase architecture.

Bitcoin OP_RETURN timestamps of each release SHA-256 are published via the OriginStamp and OpenTimestamps services, providing public, externally-verifiable proofs of priority. The two TDCommons defensive publications are released under the Creative Commons Attribution 4.0 license, with explicit patent waivers from the inventor.

1.2 Defensive publications

TDCommons #10079	"Cryptographic Identity Document System Using TOTP-Derived Symmetric Keys for Offline Issuer-Mediated Access Control", 12 May 2026. https://www.tdcommons.org/dpubs_series/10079
TDCommons #10167	"Self-Verifying Single-File Cryptographic Documents with Dual-Passphrase Architecture for Offline Recipient-Mediated Access Control", May 2026. https://www.tdcommons.org/dpubs_series/10167

© 2013–2026 Https Card — Internet Identity Card Ltd
UK Co. 09168431 · Trademark UK00003166480 · 124 City Road, London EC1V 2NX, United Kingdom

2. Core engineering innovations

2.1 Single self-contained executable file

The entire generator and every exported card are single HTML files (200–300 KB) that embed: HTML structure, CSS styling, JavaScript runtime, the hash-wasm Argon2id WebAssembly library, and where applicable the encrypted identity payload. No external scripts, no CDN dependencies, no service workers, no installation.

2.2 Dual-passphrase architecture (v8.4)

Version 8.4 introduces a clean separation between the issuer's long-lived secret (Memorable Word, never shared) and the per-export Card Passphrase (auto-generated, shared with recipient on a separate channel). This protects the issuer's vault and signature key even when many cards are distributed.

2.3 Argon2id memory-hard derivation (v8.4)

The migration from iteration-based KDFs to Argon2id at 96 MiB is, to our knowledge, the first deployment of a memory-hard KDF in a fully-offline single-file identity artefact that runs on commodity browsers via WebAssembly. The parameters are tuned to remain usable on mid-range mobile devices while raising the cost of offline brute force by multiple orders of magnitude compared to PBKDF2.

2.4 Self-verifying file integrity (v8.4)

The SHA-256 page integrity scheme (Mode A) embeds, in the file itself, the hash of the file with a known placeholder. At load, the file recomputes its own hash and refuses to operate if the verification fails. This produces a self-validating artefact without any external infrastructure.

2.5 IIFE module isolation

All cryptographic primitives are wrapped in an Immediately-Invoked Function Expression that exposes only the public API (D for decryption). Internal helpers (_zeroize, _ctEq) are not accessible from the global scope, reducing the attack surface for prototype-pollution or extension-based interference.

2.6 Quick-mode auto-render (v8.4)

Quick Cards reuse the full Secure-Card structure (3D flip, integrity check, footers) but inject the identity directly into the page rather than encrypting it. A primary render path hijacks _iic.D to return the embedded data through uI() (reusing all the styling code of Secure Cards), and a fallback inline renderer guarantees a usable artefact even under degraded WebCrypto/WebAssembly conditions.

3. Immutability & regulatory implications

3.1 Technical basis for immutability

A v8.4 card is immutable because:

© 2013–2026 Https Card — Internet Identity Card Ltd
UK Co. 09168431 · Trademark UK00003166480 · 124 City Road, London EC1V 2NX, United Kingdom

1	**SHA-256 of the file**	is embedded and self-verified at load.
2	**AAD-bound ciphertext**	cannot be moved between cards (per-CID AAD).
3	**ECDSA signature (Secure)**	binds the identity payload to the issuer's signing key.
4	**Fresh CID per export**	each export instance is distinguishable from any other.

3.2 Consequences for the issuer

Once a card is exported and shared, the issuer cannot modify it. A correction means producing a new card with a new CID. Old cards remain valid until they expire, are individually rejected by the issuer, or are superseded by a published revocation list (out of scope for v8.4).

3.3 Use cases enabled

✓	**KYC snapshots**	A regulated entity can capture an identity at a precise moment with audit-grade integrity.
✓	**Time-bound proofs**	Short-lived (m5/m15/m30/h1) cards for ephemeral access tokens, payment confirmation links.
✓	**Evidence-grade records**	Documents and credentials with embedded integrity for legal or compliance contexts.
✓	**Professional credentials**	Diplomas, memberships, certifications that the recipient can verify offline.
✓	**Self-sovereign business cards**	Quick Cards as portable, verifiable vCards that can be shared without any platform.

3.4 Regulatory framework alignment

GDPR (EU 2016/679)	Data minimization, storage limitation, integrity (Art. 5(1)f). IIC issuer holds the data; no third party is involved.
eIDAS 2.0	IIC is positioned as a self-sovereign artefact complementary to qualified eID schemes, not a substitute for them.
UK GDPR & DPA 2018	Identical to EU GDPR principles; UK ICO guidance on self-hosted identity tooling applies.
NIST SP 800-63-3	IIC corresponds to IAL1 (self-asserted) when used without external corroboration. Higher IALs require external verifiers.

© 2013–2026 Https Card — Internet Identity Card Ltd
UK Co. 09168431 · Trademark UK00003166480 · 124 City Road, London EC1V 2NX, United Kingdom

FIPS 180-4 & SP 800-38D	SHA-256 and AES-GCM primitives match NIST specifications via WebCrypto.

4. Standards compliance

4.1 Cryptographic standards

RFC 9106	Argon2 password hashing function
NIST SP 800-38D	AES-GCM authenticated encryption
NIST FIPS 180-4	SHA-256 secure hash
NIST FIPS 186-4	ECDSA digital signature with P-256 curve
NIST SP 800-132	PBKDF2 password-based key derivation
RFC 6238	TOTP time-based one-time password (legacy v8.3 feature, retained for backward compatibility)

4.2 Browser compatibility matrix

Browser	Minimum version
Chrome / Chromium	88 (WebCrypto + WebAssembly + aspect-ratio)
Firefox	89 (best file:// behaviour)
Safari	15 (WebCrypto fully complete)
Brave	matches Chromium baseline
Edge	90 (Chromium-based)
Mobile Safari	iOS 15 +
Mobile Chrome	Android 8 + (WebAssembly required)

5. Change history

v6 (2023)	First public single-file generator. PBKDF2-SHA-256, AES-GCM, TOTP gate.
v8.0 (2025)	Dual-domain key architecture, immutability properties, identity score.
v8.3 (2025)	TOTP secret obfuscation, IIFE isolation, expanded threat model, TDCommons defensive publication #10079.

© 2013–2026 Https Card — Internet Identity Card Ltd
UK Co. 09168431 · Trademark UK00003166480 · 124 City Road, London EC1V 2NX, United Kingdom

v8.4 (2026)	Argon2id KDF migration, dual-passphrase architecture, SHA-256 page integrity, Quick-mode auto-render, short-lived expirations, paste normalization, compact UX (collapsible integrity, merged footer, legal footer).
v8.4.1 (2026)	Documentation update: TDCommons defensive publication #10167 referenced; timeline corrected (httpscard.com 2013, internetidentitycard.com 5 January 2014, trademark filing 25 May 2016).

6. Issuer information

Https Card — Internet Identity Card Ltd
Company number: 09168431 (England & Wales, incorporated 2014)
Trademark: UK00003166480 (filed 25 May 2016)
Domain: internetidentitycard.com (registered 5 January 2014, continuation of httpscard.com used since 2013)
Registered office: 124 City Road, London EC1V 2NX, United Kingdom
Contact: via the official website.

Open defensive publications (CC BY 4.0):
• TDCommons #10079 — https://www.tdcommons.org/dpubs_series/10079
• TDCommons #10167 — https://www.tdcommons.org/dpubs_series/10167

© 2013–2026 Https Card — Internet Identity Card Ltd
UK Co. 09168431 · Trademark UK00003166480 · 124 City Road, London EC1V 2NX, United Kingdom