USER GUIDE

version 8.4.1

INTERNET IDENTITY CARD ™

How to create, share, and verify your offline Internet Identity Card

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.

1. Welcome

Internet Identity Card ™ (IIC) is a universal Internet Identity Card you create and control yourself. Unlike services that store your data on remote servers, IIC is a single self-contained HTML file (about 336 KB) that runs entirely on your device. No account, no installation, no internet connection required after the file is downloaded.

What v8.4 brings

Version 8.4 introduces a new dual-passphrase architecture that strengthens the cryptography and improves the sharing model:

1	**Argon2id**	Modern memory-hard key derivation (96 MiB, t=4, p=4) replaces the older iteration-based approach. Resists GPU and ASIC cracking far better.
2	**Card Passphrase**	Every exported card now uses its own auto-generated, high-entropy passphrase. The original Memorable Word stays in the vault on your device.
3	**SHA-256 page integrity**	Each exported card carries its own SHA-256 hash. The card verifies itself when opened and refuses to work if it was tampered with.
4	**Quick & Secure modes**	Quick cards display identity instantly with no passphrase. Secure cards add encryption, encrypted messages and digital signatures.
5	**Short-lived expirations**	In addition to days and months, you can now expire a card in 5, 15 or 30 minutes, or 1 hour, useful for time-bound proofs.
6	**Refreshed UI**	A compact integrity status, a new photo placeholder, paste-friendly passphrase inputs and a cleaner footer.

2. Creating your identity card

Step 1 — Open the generator

Download the generator HTML file from internetidentitycard.com and open it in a modern browser (Chrome, Brave, Firefox, Edge). No installation is required.

Step 2 — Choose a mode

Quick Card	Identity visible directly when the card is opened. Best for public business cards, social profiles and contact sharing.
Secure Card	Identity encrypted with a Card Passphrase. Best when only a specific recipient should see the content. Adds encrypted messages and digital signatures.

Step 3 — Fill in your details

IIC supports up to 27 identity fields: name, date of birth, nationality, photo, multiple phone numbers and addresses, more than ten social handles, payment addresses (BTC/ETH) and free-text notes. Only what you enter is included in the card.

Step 4 — Secure mode only: create a Memorable Word

If you chose Secure mode, you are asked to define a Memorable Word (minimum 12 characters, three character classes, not a common password). This word protects your local vault and is used as the seed for backups. **It never leaves your device.**

Step 5 — Export

Click **Export**. For Secure cards, a unique Card Passphrase of the form `aBc1-De2F-gH3i-Jk4L` is automatically generated and shown once. Save it somewhere safe — you cannot recover it from the card alone. A fresh Card Number (CID) is generated for this specific export.

Step 6 — Receive your HTML file

The generator produces an HTML file named `IIC-XXXX-XXXX-XXXX.html` where the X's are the unique CID. This single file is your portable, self-verifying identity card.

3. Sharing your card

Quick Card

Send the HTML file by email, messaging app, cloud share, USB stick, or QR code. The recipient just opens it in any modern browser — nothing else is needed.

Secure Card

You need to communicate two things:

1	**Card file**	Share the HTML file via any channel (email, cloud, USB, etc.).
2	**Card Passphrase**	Communicate the auto-generated passphrase through a **separate trusted channel** (phone call, in person, encrypted messenger). Never send the card and its passphrase together.

When recipients open the file in a browser, they see the locked card. They type the Card Passphrase, and after a 1–3 second Argon2id derivation, the identity appears. Pasted passphrases are auto-formatted with the correct hyphens.

4. SHA-256 page integrity

Every exported card embeds the SHA-256 hash of its own HTML in a meta tag. When the card is opened, the page recomputes that hash and compares it to the embedded value:

✓	**Integrity verified**	The card displays a green ✓ in the integrity panel. Everything is as the issuer published it.
✓	**Integrity failed**	The card detects a modified file. A full-screen red warning appears, all decryption controls are disabled, and the card refuses to open.
✓	**Verification unavailable**	The browser blocked the self-fetch (typically Chrome opening a local file://). The card still works, but the live check could not run. Open the file in Firefox or host it over HTTPS to enable the live check.

The full reference and live hashes are visible under "Advanced ■" in the integrity panel.

5. Card immutability

Once exported, an IIC card is immutable. Even you, the issuer, cannot edit the file you shared without breaking the integrity hash and the digital signature. To change anything, you must export a new card with a new Card Number.

This property is essential for: KYC snapshots, evidence-grade records, time-bound proofs, professional credentials, and any context where audit trails matter.

6. Security & privacy

How is my data protected?

✓	**Secure Card encryption**	AES-256-GCM with a 256-bit key derived from your Card Passphrase via Argon2id (96 MiB, 4 iterations, parallelism 4).
✓	**Backup encryption**	Backup files (.iic) are encrypted with PBKDF2-SHA-256 (600,000 iterations) using your Memorable Word, then AES-256-GCM.
✓	**Memory hygiene**	After every cryptographic operation, derived keys and plaintext buffers are zeroed out before being garbage-collected.
✓	**Constant-time comparison**	Memorable Word verification uses a constant-time comparison function to resist timing side-channels.
✓	**CSP & permissions**	Each exported card ships with a strict Content Security Policy and a Permissions-Policy that disables camera, microphone, geolocation, payment and USB access.

What about my Memorable Word?

Your Memorable Word never leaves your device. It is used:

1	**Locally**	To unlock the vault stored in your browser's localStorage.
2	**For backups**	As the seed to encrypt backup files (.iic) you can store on a USB drive or in the cloud.
3	**To sign**	When you use the Sign feature, the private signature key is unlocked with the Memorable Word.

7. Frequently asked questions

Question	Answer
Can I edit a card after exporting it?	No. Cards are immutable. Edit your identity in the generator and export a new card.
What happens if I lose my Card Passphrase?	You cannot decrypt that specific exported card. Generate a new one from the generator.
What happens if I lose my Memorable Word?	Your local vault becomes unrecoverable. You must restart from a backup .iic file.
Can someone modify a card I shared?	Yes, anyone can edit an HTML file. But the SHA-256 integrity check will detect the modification and refuse to open the card.
Does the card need internet to open?	No. After download, the card runs fully offline. The only optional network request is the self-fetch for integrity verification.
Which browsers are supported?	Chrome 88+, Brave, Firefox 89+, Edge 90+, Safari 15+. WebCrypto and WebAssembly are required.
Can I revoke a card I shared?	Not in the traditional sense. You can set an expiration date, and you can stop honoring old cards yourself. Each export has a unique Card Number for tracing.
Is my identity uploaded anywhere?	No. The generator runs entirely in your browser. No telemetry, no analytics, no servers.

8. About us

Https Card — Internet Identity Card Ltd is a UK company (No. 09168431, incorporated 2014) based in London, holder of the UK trademark UK00003166480 (filed 25 May 2016) and the domain internetidentitycard.com (registered 5 January 2014, continuation of the inventor's earlier domain httpscard.com used since 2013). The IIC project is the product of more than a decade of research on

offline identity and self-sovereign cryptographic artefacts.

Open defensive publications

The IIC architecture is documented in two open defensive publications on Technical Disclosure Commons (Elsevier), released under the Creative Commons Attribution 4.0 license:

• TDCommons **#10079** (12 May 2026) — TOTP-derived symmetric keys for offline issuer-mediated access control.
https://www.tdcommons.org/dpubs_series/10079

• TDCommons **#10167** (May 2026) — Self-verifying single-file documents with dual-passphrase architecture.
https://www.tdcommons.org/dpubs_series/10167

Get in touch

Website: internetidentitycard.com
Address: 124 City Road, London EC1V 2NX, United Kingdom