USER GUIDE

version 9.0

INTERNET IDENTITY CARD ™

Creating, using & sharing your Internet Identity Card

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. Welcome

Your Internet Identity Card (IIC) is a single file that belongs entirely to you. It works without any server, account, or internet connection: everything happens inside the file, in your browser. Your identity data is encrypted with your passphrase, and nobody — including us — can read it without that passphrase.

New in version 9.0: your card's signatures are now *post-quantum ready*. In plain terms: signatures use two locks instead of one — a proven classical lock (ECDSA) and a new lock (ML-DSA) designed to resist future quantum computers. A document signed today stays provably yours even in a future where quantum computers exist.

2. Creating your card

- **Quick card** — instant, unencrypted, for low-stakes sharing of basic contact info.
- **Secure card** — protected by your **Memorable Word** (minimum 12 characters), chosen at creation. Your data is encrypted with AES-256 and a key derived from it using Argon2id (a modern, memory-hard method that makes password-guessing attacks extremely expensive).

Choose a Memorable Word you can remember but others cannot guess. **There is no reset.** If you lose it, the data cannot be recovered — by design, since no one else holds a key. When you export a Secure card for someone else, the app generates a separate **Card Passphrase** (format aBc1-De2F-gH3i-Jk4L) that encrypts that exported copy; you share it with the recipient through a channel you trust.

When you create a secure card, version 9.0 also generates your signing keys (both the classical and post-quantum ones) automatically. You don't need to do anything: it just happens, and your backups include them.

3. Sharing your card

- Export produces a standalone file you can send by any channel you trust.
- The exported card verifies itself: if anyone alters even one character of the file, it locks itself down and shows a tampering warning.
- The exported card can also *verify signed documents* completely offline — it carries its own verification engine inside.

4. Signing documents with your card

Your card can sign texts and files, producing a *receipt* — a small block of text that proves the exact content existed and was signed by your card at a given time. Signing requires your Memorable Word, so only you can sign. Receipts chain together, so a sequence of signatures cannot be silently reordered or trimmed.

In version 9.0, every receipt carries the two signatures (classical + post-quantum). Anyone with your card file — or any v9 card — can paste the receipt into the verify panel and check it offline. If the content was tampered with, verification fails.

5. The SHA-256 integrity check

Every exported card displays its own SHA-256 fingerprint — a unique code that changes if anything in the file changes. You can publish or share this fingerprint separately (for example, in an email or on your website), so recipients can confirm the file they received is exactly the one you sent.

6. Immutability & blockchain anchoring

Your card cannot be modified after export without breaking its self-check. For stronger, date-stamped proof, a card or package fingerprint can be anchored on the Bitcoin and Ethereum blockchains: this proves the file existed at that date, without revealing any of its contents, and without trusting any company or authority.

7. Security & privacy at a glance

- Your data never leaves your device — there is no server.
- Encryption: AES-256-GCM; key derived with Argon2id from your passphrase.
- Signatures: hybrid classical + post-quantum (ECDSA P-256 + ML-DSA-65).
- Integrity: SHA-256 self-verification, working fully offline.
- The card asks for no permissions: camera, microphone, and location are disabled by policy.

8. Frequently asked questions

What does “post-quantum ready” actually mean?

Today's signatures rely on math that a large future quantum computer could break. Your v9 card adds a second signature based on different math (standardized by NIST as FIPS 204 / ML-DSA) that is designed to resist quantum attacks. Both signatures must match for a document to verify — so even if the classical one is broken someday, your documents remain provably yours.

Do I need internet to verify something?

No. Creation, signing, and verification all work offline. That's the point of the IIC.

What if I lose my card file or passphrase?

Keep encrypted backups (the app can export one). The passphrase itself has no recovery: no one can reset it, because no one else has it.

Are my old cards and receipts still valid?

Yes. Version 9.0 verifies everything v8 produced. New signatures simply carry the extra post-quantum component.

9. About us

Https Card — Internet Identity Card Ltd · UK Companies House No. 09168431 · 124 City Road, London EC1V 2NX, United Kingdom · Trademark UK00003166480 · internetidentitycard.com. © 2013–2026.