USER GUIDE

version 10.0

INTERNET IDENTITY CARD ™

Creating, opening, sharing & signing

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 · #10795 · #10796 · #11121 (CC BY 4.0)

This document supersedes the v9.0 edition. Two things changed for you: your card now asks for your memorable word every time you open it, and you are given a recovery phrase that you must keep. Both are explained in Sections 3 and 4, and both exist because of what was wrong before.

IIC v10.0 is a corrective release. It introduces no new capability: it repairs six defects found in the v9.0 implementation, four of which were reachable in normal use. Section references to v9.0 behaviour are retained where a reader of the previous edition would otherwise be misled.

1. What changed, and why

Until v10.0, the key that encrypted your identity was kept in your browser alongside the encrypted data itself. Your card opened without asking for anything, which was convenient — and it meant that anyone who could read your browser profile could decrypt your identity and use your signing key. Your data was encrypted, but the key that opened it sat next to it, so no password was needed — only access. Malware running as you, a shared computer, a disk backup: any of those was enough.

v10.0 removes that key. Nothing stored on your device can open your card any more. The key is rebuilt from your memorable word each time, which is why you are now asked for it, and why opening takes a moment longer. That pause is the protection working.

2. Creating your card

- Open the file. No installation, no account, no network connection.
- Enter your details. They never leave your device.
- Choose a memorable word of at least twelve characters. It encrypts everything.
- Write down the recovery phrase you are shown, or download it. See Section 3.
- Your card is created locally and can be exported as a standalone file.

3. Your recovery phrase

At setup you are shown a phrase of six blocks of four characters. It opens your card if you forget your memorable word. It is displayed once, it is not stored anywhere, and it cannot be reissued or recovered by anyone — not by us, because we never had it.

- Write it down, or use the download button, before continuing.
- Keep it somewhere other than the device holding your card. A phrase saved in the same browser as the card it protects defends against nothing.
- If you created your card without a memorable word, the phrase is the **only** way in. The card tells you so at the moment it shows the phrase.

Losing your memorable word is now recoverable. Losing both the word and the phrase is not, by anyone, under any circumstances. That is the price of an identity nobody else holds a copy of.

4. Opening your card

Each time you open the card, enter your memorable word. If you have forgotten it, choose “I lost my memorable word” and enter your recovery phrase instead.

If you were using a card created before v10.0, the first opening asks you to set this up: it shows your recovery phrase, asks you to type it back, and only then removes the old unprotected key. Nothing is deleted until both ways in have been tested.

5. Sharing your card

- Export your card as a single HTML file.
- Send it by any means: email, messaging, USB stick, printed QR.
- The recipient opens it in any browser. No account, no software, no connection required.
- Each exported card carries its own passphrase, separate from your memorable word.

6. Signing documents

Your card can sign documents. Each signature produces a receipt carrying both a classical and a post-quantum signature, and each receipt is linked to the one before it.

If signing is refused, the card will say so and name the cause. This is deliberate. Before v10.0, a card that could not produce the post-quantum part of a signature quietly produced a classical-only receipt that looked entirely normal — you would have believed you had signed something you had not. A refusal is a fault to report, not an obstacle to work around.

7. The SHA-256 integrity check

Every card verifies itself. It contains a fingerprint of its own contents and recomputes it each time it opens. If a single byte has changed, the card locks itself and says so. This happens entirely offline, in the browser, with no server involved.

8. Immutability & blockchain anchoring

Release fingerprints are recorded on the Bitcoin and Ethereum blockchains. This proves a document existed at a given date without depending on any authority. Anchoring is performed by the issuer for each release; it is not something your card does by itself, and it cannot happen offline.

9. Security & privacy at a glance

Question	Answer
Where is my data?	On your device only. It is never transmitted anywhere.
Who can read it?	Only someone with your memorable word or your recovery phrase.
Can you recover my card?	No. We hold nothing: no copy, no key, no reset.
Is a connection needed?	No, at any point, for any function.
What if my computer is compromised?	Malware present while your card is open can reach what is open. Locking at rest protects a closed card, not an active session.

10. Frequently asked questions

Why is opening slower than before? Your key is rebuilt from your memorable word using a deliberately expensive calculation. The delay is what makes guessing your word impractical.

Can I turn off the memorable word prompt? No. Any way of opening the card without it would mean storing something that opens it, which is exactly what was removed.

Can I change my memorable word later? Not in this release. It is set once, when a card is upgraded to secure mode, and cannot be changed afterwards. If you believe it has been exposed, create a new identity rather than continuing with the existing one.

Can I get a new recovery phrase? Not in this release. The phrase is issued once, at setup. If you lose it while you still know your memorable word, your card keeps working, but you no longer have a second way in — so treat that as a reason to plan a fresh identity rather than as a minor inconvenience.

Does this change how cards are produced? No. The exported card format is unchanged: a card produced with v9.0 is produced and verified in exactly the same way.

11. About us

Https Card — Internet Identity Card Ltd, 124 City Road, London EC1V 2NX, United Kingdom. Developing the Internet Identity Card since 2013. UK Companies House 09168431.

12. Disclaimer

This document is provided for informational purposes only. It describes intended behaviour and properties under the assumptions stated in it; where those assumptions do not hold, the described protections may not apply. No software system can be guaranteed to be free of defects or completely secure. Conformance to a cryptographic standard in code is distinct from formal evaluation: nothing here constitutes a FIPS 140 CMVP validation, an ANSSI qualification, or a certification of any kind, each of which requires assessment by an accredited third party. 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).