

USER GUIDE

version 1.0 · revision 5

IIC WALLET

How to install, use, and manage your IIC cards offline

Publisher	Htps 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
Distribution	Bundled inside the IIC Complete Package (access-controlled)
Wallet size	~31 KB (single-file PWA, with manifest + service worker)
Card formats	.iic and .html (both accepted)
Companion document	IIC User Guide v10.0 — for creating cards

The Wallet software is unchanged at v1.0. It does not create, sign or modify cards, and none of the corrections made in IIC v10.0 affect it. Revision 4 corrected two cross-references: the companion guide, which still pointed at v8.4.1, and the list of defensive publications, which named two of six. Revision 5 corrects a third: the description of where the Wallet is distributed.

Where this document appears matters. *The Wallet software ships in the IIC Complete Package, an access-controlled archive. This guide is also included in the public IIC v10.0 release package for reference, and **that package does not contain the Wallet software**. Section 2 describes installation from the Complete Package; if you obtained this guide with the v10.0 release package, you have the documentation and not the application.*

Important notice — legal & usage disclaimer

Nature of the product. The IIC Wallet is an optional companion application to the Internet Identity Card (IIC) generator. It is a single-file Progressive Web App (PWA) that lets users collect and open IIC cards offline. The Wallet itself does not create, sign, or modify cards; it only opens cards that have already been issued by the IIC generator.

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

Distribution disclaimer. The IIC Wallet is distributed exclusively inside the IIC Complete Package, which is access-controlled. It is never hosted publicly. Recipients of the package are responsible for not redistributing the Wallet outside their authorised scope.

Storage disclaimer. The Wallet stores card files locally in the browser's IndexedDB. Data persists only on the device where it was added and is not transmitted anywhere. Clearing the browser's site data will remove all Wallet contents permanently.

Security disclaimer. No software system can be guaranteed to be completely secure. The protections described in this document substantially reduce — but do not eliminate — the risk of misuse, file tampering, or spoofing. Users remain responsible for the operational security of their own devices, browsers, and source files.

1. Welcome

The IIC Wallet is an optional offline application that lets you collect and open your Internet Identity Cards in one place. It runs entirely in your browser, stores nothing on any server, and works without an internet connection. The Wallet is a single-file PWA (~31 KB) shipped with a small manifest and service worker for offline support and optional installation as a native-feeling app.

Feature	What it means
Zero server	Everything runs locally in your browser. Nothing is uploaded or shared.
Works offline	After first launch, the Wallet works without any network connection.
IndexedDB storage	Cards are kept in your browser's local database, isolated per device.
Multi-format input	Accepts both .iic and .html card files via drag-drop or file picker.
Spoof-resistant	Refuses any file that does not contain the four structural IIC markers.
Cross-platform	Same experience on iPhone, Android, macOS, Windows and Linux.

2. Installing the Wallet

The Wallet is delivered inside the IIC Complete Package, the same controlled archive that contains the generator. Once you have received the package, you have two ways to use the Wallet: open it locally on your computer, or install it as a native-feeling app from your own private HTTPS server.

- **Step 1 — Receive the Complete Package.** Request access by contacting demo@internetidentitycard.com. After approval, you will receive a single ZIP archive containing the generator, the official PDF documentation set, the Wallet, and a SHA256SUMS checksum file. The public v10.0 release package is a different distribution and contains the generator and the documentation only.
- **Step 2 — Extract the wallet folder.** Unzip the package. You will find a `wallet/` folder containing six files: `iic-viewer.html` (the PWA), `manifest.webmanifest`, `sw.js` (service worker), `index.html` (a redirect), `.htaccess` (Apache config for self-hosting), and `README.md`.
- **Step 3 — Choose your usage path.** *Local use:* open `wallet/iic-viewer.html` directly in any modern browser; it works immediately without installation. *Self-hosted PWA:* upload the `wallet/` folder to an HTTPS server you control, and the Wallet becomes installable as a native-feeling app on desktop and mobile.

iOS limitation. Apple does not allow Progressive Web Apps to be installed from local files. To use the Wallet on iPhone or iPad, you must self-host it on an HTTPS server. This is an OS-level restriction that applies to every web-based app.

3. First launch — the consent dialog

When you open the Wallet for the very first time, a dialog titled “Before you continue” appears. This is a one-time disclosure of how the Wallet handles your data, written in the style of a GDPR notice. You must read it, tick the consent checkbox, and click **Accept and continue** before the Wallet activates.

- **Zero server.** The Wallet runs entirely in your browser. Nothing is uploaded, transmitted, or shared with any third party.
- **Local storage only.** Cards you add are stored in your browser's IndexedDB on this device. They never leave the device.
- **No tracking.** No analytics, no cookies, no telemetry.
- **You stay in control.** You can remove any card at any time, and clear all data via your browser's site-data settings.

After you accept, the consent is recorded in your browser's localStorage under the key `iic-wallet-consent-v1`. The dialog will not appear again on the same browser unless you clear site data or use a different browser. If the disclosure ever changes substantially, the key version number is incremented and consent is requested again.

Revoking consent. Open your browser's developer tools or site settings, navigate to the Wallet's origin, and delete the `iic-wallet-consent-v1` entry from localStorage. On the next reload, the dialog reappears. Clearing all site data for the Wallet origin also removes all your stored cards.

4. Adding cards to the Wallet

- **Drag and drop.** Drag any IIC card file onto the Wallet window. Works on desktop browsers.
- **File picker.** Click **Choose card file** on the empty-state screen, or **+ Add card** in the header. This is the only method available on iPhone.
- **Auto-open via the .iic extension.** If you installed the Wallet as a PWA on a Chromium-based browser, the operating system registers it as the default handler for .iic files.

Why .iic and not .html? If the Wallet registered itself as the handler for .html, it would capture every HTML file on your system. The custom extension lets the OS open IIC cards in the Wallet without affecting any other HTML file.

Duplicate detection. If you add a card whose CID is already in your Wallet, a confirmation dialog asks whether to replace the existing entry. This lets you update a card to a newer version while keeping the same identity.

5. Opening cards

Click any card to open it. The Wallet creates a temporary blob URL and opens the card in a new browser window or tab. Each card runs in its own isolated context, with full security checks active.

Stage	What happens
Re-verification	The Wallet re-checks that the stored CID still matches the embedded CID in the card content. Any tampering since ingestion is caught here.
Blob URL creation	The card content is wrapped in a Blob and given a temporary blob: URL. The original file on disk is never modified.
New window	The card opens in a new tab or PWA window. All its own security mechanisms — SHA-256 integrity check, anti-rewrite verification, CSP — activate normally.
URL revocation	After 60 seconds the blob URL is revoked to free memory. The card stays loaded for as long as you keep its window open.

Pop-up blocker. Some browsers block `window.open()` calls that are not the direct result of a click. The Wallet calls it inside the click handler, so this normally works. If a card refuses to open, allow pop-ups for the Wallet's origin.

6. Removing cards & managing your Wallet

Hover over a card in the grid, or long-press on touch devices, to reveal a small red X in the top-right corner. A confirmation dialog appears before removal.

The original file is not deleted. Removing a card from the Wallet only deletes the copy stored in the browser. The original .iic or .html file on your disk is unchanged.

Browser	Clearing all Wallet data
Chrome / Edge	Settings → Privacy and security → Site settings → View permissions and data stored across sites → Wallet origin → Clear data.
Firefox	Settings → Privacy & Security → Cookies and Site Data → Manage Data → Wallet origin → Remove.
Safari (desktop)	Preferences → Privacy → Manage Website Data → Wallet origin → Remove.
Safari (iPhone)	Settings → Safari → Advanced → Website Data → swipe left on the Wallet origin → Delete.

7. Security model — six layers of defence

The Wallet adds defensive layers on top of the cryptographic protections that each IIC card already carries. The combination yields six independent checks, each of which can independently refuse a card.

Layer	Check
Multi-marker validation	At ingestion, the Wallet rejects any file that does not contain all four IIC structural markers: integrity meta tag, hash comment, flip-card DOM structure, and CID declaration.
CID / filename match	If a card's filename contains a CID pattern that does not match the embedded CID, the Wallet refuses the file and shows a blocking dialog.
Re-verification before opening	Every time you click a card, the Wallet re-checks the stored CID against the live content, catching any tampering of the IndexedDB between ingestion and opening.
Per-card SHA-256 integrity	Each card carries its own SHA-256 hash and verifies itself when opened. Any byte modification triggers a full-screen fail-closed lockdown.
Anti-rename verification	The card itself also checks that its filename CID matches its embedded CID, preventing identity-swap attacks even when the Wallet is not in the loop.
Cryptographic encryption	Secured cards encrypt their contents with AES-256-GCM under a key derived from the passphrase via Argon2id (RFC 9106, 96 MiB, t=4, p=4). The Wallet never sees this content.

The Wallet does not verify signatures. Cards issued with a hybrid ECDSA P-256 and ML-DSA-65 signature carry their own verification engine and check themselves when opened, independently of the Wallet.

8. Troubleshooting

Symptom	Cause and action
"Not a valid IIC card"	The file does not contain the four required IIC markers. Verify it with the internetidentitycard.com/verify tool.
"Card refused: filename mismatch"	The filename contains a CID different from the one embedded in the card. Rename the file back to its original name. If you do not trust the source, do not add the file.
"Pop-up blocked"	The browser blocked the new window. Allow pop-ups for the Wallet's origin, then click again.
Card does not appear after adding	The file exceeds 2 MB, or the browser denied IndexedDB access. Check the console, and ensure you are not in a private window.
The Install button does not appear	The Wallet is served from file:// or from a non-HTTPS origin, or it is already installed.
On iPhone, .iic files do not open in the Wallet	iOS does not allow third-party apps to register as default handlers. Open the Wallet manually and use the file picker. This cannot be worked around on iOS.

9. Frequently asked questions

Question	Answer
Where are my cards stored?	In your browser's IndexedDB, on the device where you added them.
Can I sync across devices?	No. Add the card files manually on each device.
What if I clear browser data?	All cards in the Wallet are deleted. The original files on your disk are not affected.

Why both .iic and .html?	The two hold identical content. .iic exists so the Wallet can auto-open it without interfering with regular HTML files.
Can the Wallet read secured cards?	No. They are encrypted with AES-256-GCM under a passphrase-derived key. The Wallet stores and forwards the encrypted blob only.
Why not on the App Store?	By design. The Wallet is access-controlled and distributed only inside the IIC Complete Package.
Can I export my Wallet?	Each stored card is a copy of the file you added. Re-use the originals, or back up IndexedDB via developer tools.
What if I lose the device?	The card files remain. Add them again to a new Wallet on another device.

10. Get in touch

Website	internetidentitycard.com
Email	demo@internetidentitycard.com
Office	124 City Road, London EC1V 2NX, United Kingdom
Company	Htpps Card — Internet Identity Card Ltd
Companies House	UK 09168431
Trademark	UK IPO UK00003166480 (2016)

11. Open defensive publications

The IIC architecture is documented in six open defensive publications on Technical Disclosure Commons, released under the Creative Commons Attribution 4.0 licence. Revision 4 of this guide corrects an earlier statement that named only the first two.

Reference	Subject
#10079 (12 May 2026)	TOTP-derived symmetric keys for offline issuer-mediated access control
#10167 (19 May 2026)	Self-verifying single-file documents with dual-passphrase architecture
#10394 (7 June 2026)	Composite defence-in-depth architecture for self-verifying cryptographic documents
#10795 (July 2026)	Canonical multi-zone neutralisation for self-serialised documents
#10796 (July 2026)	In-file stapled freshness: hash-chain validity tokens
#11121 (22 July 2026)	Post-quantum ready, offline-verifiable digital identity credential: hybrid ECDSA P-256 and ML-DSA-65 signing

Each is available at https://www.tdcommons.org/dpubs_series/<number>.

Companion documents. This guide covers the Wallet. For creating IIC cards, see the IIC User Guide v10.0. For cryptographic specifications, see the Technical Specification v10.0. For system architecture, see the Engineering Specification v10.0. For threat analysis, see the Threat Model v10.0. © 2013–2026 Htpps Card — Internet Identity Card Ltd.