

USER GUIDE

version 1.0

IIC WALLET

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

Publisher	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
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 v8.4.1 — for creating cards

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 Https 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.

Six features at a glance

1	Zero server	Everything runs locally in your browser. Nothing is uploaded or shared.
2	Works offline	After first launch, the Wallet works without any network connection.
3	IndexedDB storage	Cards are kept in your browser's local database, isolated per device.
4	Multi-format input	Accepts both <code>.iic</code> and <code>.html</code> card files via drag-drop or file picker.
5	Spoof-resistant	Refuses any file that does not contain the four structural IIC markers.
6	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 four official PDF documents, the Wallet, and a SHA256SUMS checksum file.

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 <code>wallet/iic-viewer.html</code> directly in any modern browser. The Wallet works immediately without any installation. Best for desktop and quick one-time use.
Self-hosted PWA	Upload the <code>wallet/</code> folder to an HTTPS server you control (your own domain, a private VPS, or a sub-domain). The Wallet then becomes installable as a native-feeling app on desktop and mobile. Required for iPhone use.

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.

What you are consenting to

1	Zero server	The Wallet runs entirely in your browser. Nothing is uploaded, transmitted, or shared with any third party.
2	Local storage only	Cards you add are stored in your browser's IndexedDB on this device. They never leave the device.
3	No tracking	No analytics, no cookies, no telemetry. The Wallet does not know you exist outside the current session.
4	You stay in control	You can remove any card at any time, and clear all data via your browser's site-data settings.

Why we ask only once

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 we ever change the disclosure substantially, the key version number will be incremented and consent will be requested again.

How to revoke 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 will reappear. Clearing all site data for the Wallet origin also removes all your stored cards.

4. Adding cards to the Wallet

Once the Wallet is open and you have accepted the disclosure, you can add IIC cards in three ways. All three accept both the `.iic` and the `.html` extensions.

Method 1 — Drag and drop

Drag any IIC card file from your file manager directly onto the Wallet window. The dropzone is highlighted in cyan while you drag. Release the mouse to add the card. This works on desktop browsers (Chrome, Edge, Firefox, Safari).

Method 2 — File picker

Click **Choose card file** on the empty-state screen, or **+ Add card** in the header. The system file picker opens. You can select one or several card files at once. This is the only method available on iPhone (mobile Safari).

Method 3 — Auto-open via `.iic` extension

If you installed the Wallet as a PWA on a Chromium-based browser (Chrome, Edge, Brave), the operating system registers it as the default handler for `.iic` files. Double-clicking any `.iic` file then opens the Wallet, ingests the card, and immediately opens it in a new window.

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 `.iic` 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 you want to replace the existing entry with the new file. This lets you update a card to a newer version while keeping the same identity. Click **Cancel** to keep both versions if needed.

5. Opening cards

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

What happens behind the scenes

1	Re-verification	Before opening, the Wallet re-checks that the stored CID still matches the embedded CID in the card content. Any tampering since ingestion is caught here.
2	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.
3	New window opening	The card opens in a new browser tab or PWA window. All its own security mechanisms (SHA-256 integrity check, anti-rename verification, CSP) activate normally.
4	URL revocation	After 60 seconds, the blob URL is revoked to free memory. The card stays loaded in its window for as long as you keep it open.

Pop-up blocker

Some browsers block `window.open()` calls if they are not the direct result of a user click. The Wallet calls `window.open()` immediately inside the click handler, so this should normally work. If a card refuses to open with the message “*Pop-up blocked*”, allow pop-ups for the Wallet’s origin in your browser settings.

6. Removing cards & managing your Wallet

Cards added to the Wallet stay until you explicitly remove them or until your browser's site data is cleared. The Wallet gives you simple, granular controls.

Removing a single card

Hover over a card in the grid (or long-press on touch devices) to reveal a small red **X** button in the top-right corner. Click it. A confirmation dialog warns you that the card will be removed from the Wallet. Confirm to remove.

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.

Clearing the entire Wallet

To remove all cards at once, clear the Wallet's site data from your browser:

Chrome / Edge	Settings → Privacy and security → Site settings → View permissions and data stored across sites → find the Wallet origin → Clear data.
Firefox	Settings → Privacy & Security → Cookies and Site Data → Manage Data → select the Wallet origin → Remove.
Safari (desktop)	Preferences → Privacy → Manage Website Data → search for the Wallet origin → Remove.
Safari (iPhone)	Settings app → 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.

1	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. Spoofed or look-alike files are refused immediately.
2	CID / filename match	If a card's filename contains a CID pattern (e.g. IIC-AAAA-BBBB-CCCC.html) that does not match the embedded CID, the Wallet refuses the file and shows a red blocking dialog.
3	Re-verification before opening	Every time you click a card to open it, the Wallet re-checks the stored CID against the live content. This catches any tampering of the IndexedDB between ingestion and opening.
4	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.
5	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.
6	Cryptographic encryption	Secured cards encrypt their contents with AES-256-GCM, using a key derived from the passphrase via Argon2id (RFC 9106, 96 MiB, t=4, p=4). The Wallet never sees this content; only the recipient with the passphrase can unlock it.

8. Troubleshooting

Common errors and dialogs, with their causes and recommended actions.

“Not a valid IIC card” toast

Cause: the file you tried to add does not contain the four required IIC markers. This usually means the file is not an IIC card, or it has been damaged. **Action:** verify the file is a genuine IIC card with the internetidentitycard.com/verify tool.

“Card refused: filename mismatch” dialog

Cause: the file's name contains a CID different from the one embedded inside the card. This may indicate that someone renamed the file with another identity's number. **Action:** rename the file back to its original name (matching the embedded CID) and try again. If you do not trust the source, do not add the file.

“Pop-up blocked” toast

Cause: the browser blocked the new window when you clicked a card. **Action:** allow pop-ups for the Wallet's origin in your browser settings, then click the card again.

Card does not appear after I added it

Cause: the file is too large (over 2 MB) or the browser denied access to IndexedDB. **Action:** check the browser console for errors, and ensure you are not in a private/incognito window that disables persistent storage.

The Install button does not appear

Cause: the Wallet is being served from `file://` or from an HTTP (non-HTTPS) origin, or you have already installed it. **Action:** serve the Wallet from an HTTPS origin to enable installation.

On iPhone, .iic files do not open in the Wallet

Cause: iOS does not allow third-party apps to register as the default handler for any file type. **Action:** open the Wallet manually, then use the file picker to add the card. This limitation cannot be worked around on iOS.

9. Frequently asked questions

Where are my cards stored?	Inside your browser's IndexedDB, on the device where you added them. They never leave your device.
Can I sync my Wallet across devices?	No. There is no synchronisation mechanism. To use the same cards on multiple devices, add the card files manually on each device.
What happens if I clear my browser data?	All cards stored in the Wallet are deleted. The original card files on your disk are not affected.
Why does the Wallet accept both .iic and .html?	The two extensions hold identical content. .iic exists so the Wallet can auto-open it on systems that support PWA file handlers, without interfering with regular HTML files.
Can the Wallet see the contents of my secured cards?	No. Secured cards are encrypted with AES-256-GCM and a key derived from the passphrase. Only the recipient who knows the passphrase can decrypt the card content. The Wallet only stores and forwards the encrypted blob.
Why is the Wallet not on the App Store or Play Store?	By design. The Wallet is access-controlled and distributed only inside the IIC Complete Package. Hosting it on a public app store would defeat that distribution model.
Can I export my Wallet contents?	Each card stored in the Wallet is a copy of the original file you added. To export, simply re-download the original file you added, or back up your IndexedDB using your browser's developer tools.
What if I lose access to the device with my Wallet?	The card files themselves remain. Add them again to a new Wallet on a different device. As long as you still have the original .iic or .html files, you can rebuild your Wallet at any time.

Get in touch

For demo requests, partnership inquiries, or to report a security issue concerning the IIC Wallet, please contact us using the channels below.

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

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

Companion documents. This guide focuses on the Wallet. For details on creating IIC cards, see the **IIC User Guide v8.4.1**. For cryptographic specifications, see the **Technical Specification**. For system architecture, see the **Engineering Specification**. For threat analysis, see the **Threat Model**. All four documents are bundled in the same Complete Package as this Wallet.