FreeholdIP

Issuing credentials — a guide for issuers

FreeholdIP lets government agencies, boards, associations, and schools issue licenses, certifications, and diplomas that the recipient and — credentials that can't be faked, work offline, and keep proving themselves even if you're gone. You stay the trust root: every credential is signed with *your* key and verifies against *your* identity and domain.

How it works, in one paragraph

You sign a credential with your institution's key, and issue it to the recipient's own FreeholdIP identity. They own it; you never see their key, and they never see yours. Anyone they show it to can verify it instantly — against the digital signature key published at your identity on the public record and, once you've published a single DNS record, against your own domain. You can renew or revoke any credential at any time, for free.

Step 1 — Become a verified issuer

1. Tell us about your organization and authorized representative, prove control of your official domain (a one-line DNS TXT record we give you), and upload proof of your authority to issue.
2. Verified issuers are the trust root of the whole system, so this gate is deliberate.
3. You generate your digital signature key — we never receive it — and download a device login file and a recovery sheet. We then put your issuer identity on the public record (we cover that cost).
4. Add one DNS TXT record. This is what makes a credential verify as Whoever controls your domain *is* you — FreeholdIP is not in the trust path. (Until you publish it, credentials still verify as authentic, just marked "recognized issuer, domain not yet verified.")

Guard your device login file and recovery sheet. Your digital signature key is your institution’s identity. Keep the device login file and its recovery sheet safe — anyone with them can sign as you, and if you lose both the key and the recovery sheet, you’d need to re-onboard a new identity.

Step 2 — Sign in to your portal

Go to your Issuer Portal and enter your and your (upload your device login file the first time on a new device). Your key is unlocked — we never hold it. You’ll see your organization name and a “✓ Verified issuer” badge at the top, and a confirmation that your digital signature key is ready.

Step 3 — Issue a credential

The holder creates *their* FreeholdIP identity first and gives you their . In the tab, fill in:

- Holder name, and (optionally) a sealed into the credential so it can't be swapped without breaking verification — you vouch it's the right person (FreeholdIP doesn't identity-check it).
- Credential type, an optional number, the title/award, and jurisdiction.
- An — or mark it if it never expires.
- Optionally, a certificate document (PDF/image) the holder keeps.
- The holder’s address or identity name.

Click . The credential is signed in your browser, issued to the holder’s identity, and is immediately verifiable. You never handle the holder’s key, and they own the credential the moment it’s issued.

Step 4 — Manage credentials

In the tab, search your issued credentials, then:

- — extend a credential’s expiry.
- — mark it revoked.

- — bring a revoked credential back.

These re-point the credential — — and the change shows up immediately to anyone who verifies it.

You can’t “edit” a credential’s content — and that’s the point. Because each credential is sealed with a tamper-proof digital signature, its details can’t be silently altered (that’s what makes it trustworthy). To correct content, simply revoke it and issue a corrected replacement.

Step 5 — Looking after your signing key (and replacing it)

Your digital signature key is like your institution’s : everything you issue is sealed with it, and that seal is what proves a credential genuinely came from you. From time to time you’ll want to swap that seal for a fresh one — this is called your key. You do it yourself, in your browser, from the panel of your portal. As always, the new key is created on your device and we never see it.

The console asks you *why* you’re rotating, because there are two very different situations and the difference matters a lot:

1 · Routine replacement — simply good housekeeping

Choose Nothing breaks: every credential you’ve already issued , because each one carries a secure, tamper-proof timestamp showing it was signed *before* you retired the old key. From now on, new credentials are sealed with the new key. Good times to do this:

- — about is plenty for most organizations. There’s no hard rule; think of it as periodically changing the locks. If you’ve never rotated and it’s been a few years, now is a fine time.
- — a staff member, a contractor, or an IT vendor who could have touched the key or its login file.
- — for example onto a new, locked-down computer.

2 · You think your key may be exposed — act right away

Choose This is the urgent case. Unlike a routine rotation, it — on purpose. The reason: if someone else may have a copy of your key, there’s no way to tell

which credentials are really yours and which are forgeries, so all of them have to be treated as suspect. You then under the new key. Treat your key as compromised if:

- Your was lost, stolen, emailed, photographed, or left on a shared or unsecured computer.
- A computer that ever held your key was .
- You notice appearing under your name.
- A false alarm just costs you a little re-issuing; a real compromise you ignore can mean fraud committed in your name.

One finishing step: update your domain. Right after you rotate, the console shows you the one-line DNS record to publish for your new key (and, in the compromise case, the old record to remove). Publishing it is what keeps the **“✓ Verified by yourdomain.org”** badge — your domain is the real proof of who you are, so it has to point at your current key. The console spells out exactly what to add. For a planned rotation, leave the old record in place too, so credentials you issued earlier stay domain-verified.

You need your current key to rotate. A rotation is authorized by your *existing* key approving the new one — and that’s precisely why no one else, **not even FreeholdIP**, can swap your key out from under you. So if you still have your key, rotate while you do. If you’ve completely lost it, restore it first from your **recovery sheet**, then rotate. If both the key and the recovery sheet are gone, contact us to re-establish your identity.

Why people can trust it

Every credential verifies against the digital signature key published at *your* identity on the public record, and — once you’ve published your DNS record — against *your own domain*. A forgery (anything signed by a key that isn’t yours) is rejected automatically. Verification needs no account and no fee, works offline, and keeps working — your authority lives in your key and your domain, not in us.

Quick answers

What does it cost us to issue?

Becoming a verified issuer and issuing, renewing, or revoking credentials are free to you — we cover the cost of recording your issuer identity. Each member needs their own FreeholdIP identity (a small one-time fee they pay).

Do recipients need anything first?

Yes — a FreeholdIP identity. They create it themselves and give you their address or identity name; then you issue to it.

Can we change a credential after issuing it?

You can renew, revoke, or reinstate it freely. You cannot alter its content — to correct content, revoke and re-issue a replacement.

How often should we rotate (replace) our signing key?

For routine hygiene, about once a year is plenty — or whenever someone with access leaves. Choose and nothing breaks: every credential you've already issued keeps verifying. But if you ever suspect your key was exposed or stolen, don't wait for a schedule — rotate immediately and choose See *Step 5* for the difference and what each one does.

Can we affect a holder's identity or another issuer's credentials?

No. You manage only the credentials you issue. Holders own their identities; other issuers own theirs.

What happens to issued credentials if we ever leave FreeholdIP?

They keep verifying. They prove themselves against your identity on the public record and your domain — permissionless, public, and independent of us.

An internet you own instead of rent. FreeholdIP — a product of RaptorLockIP™.

Home Holder guide Issuer guide Terms Privacy Contact