

Renew credentials

Credentials expire. When one expires, the node no longer uses it, and the care organization can't register on the Discovery Service or get access tokens anymore. Renew them in time.

What to renew, and when

What	When	How
X509Credential	Before the UZI server certificate expires, or when it's replaced or revoked	Create a new one from the renewed certificate (see "Get an X509Credential from a UZI certificate")
Self-issued credentials	Before their <code>expirationDate</code>	Issue a new one (see "Obtaining credentials")
Credentials from a trusted third party	Before they expire	Ask the issuer for a new one
Discovery Service registration	Never: the node refreshes it by itself	—

Keep a list of expiry dates per care organization, or check them regularly (see "Find expiring credentials" below).

Replace a credential

1. Load the new credential into the wallet (see "Load the credential into the wallet").
2. Remove the old credential from the wallet, so the node doesn't pick it by mistake:

```
DELETE <internal Nuts interface>/internal/vcr/v2/holder/<subject ID>/vc/<credential ID, URL-encoded>
```

Find the credential ID (`id`) by listing the wallet: `GET <internal Nuts interface>/internal/vcr/v2/holder/<subject ID>/vc`.

The node uses the new credential right away for new access tokens. It uses it for the Discovery Service registration at the next refresh. To update the registration right away, call the registration `POST` again (see "Register on the Discovery Service").

Find expiring credentials

List the wallet and look at each credential's `expirationDate` (or `exp` for credentials in JWT form):

```
GET <internal Nuts interface>/internal/vcr/v2/holder/<subject ID>/vc
```

This only returns valid credentials: expired ones are left out.

Revision #1

Created 2026-10-27 15:13:33 UTC by Rein Krul

Updated 2026-10-27 15:13:55 UTC by Rein Krul