Credential Trust

Authentication on Nuts heavily depends on trusted credential issuers: any attribute, relevant to the security model of the use case should be verifiable. E.g., if a party claims to be a care organization, it should be able to present a Verifiable Credential to prove it. The same applies to a user presenting their name or claiming to be a care professional.

Who should be the trusted issuer for a specific Verifiable Credential depends on the context. But generally, issuers are authoritative registries (e.g. Dutch CIBG) or even state-issued (PID of natural persons).

Credential types are defined in the credential catalog. It is the normative source for credential definitions.

Where trust is configured

- **Spec v2:** the use case decides which issuers it trusts. It sets this in the presentation definitions of its Discovery Service definition and its access policy. For example, an X509Credential is trusted by the fingerprint of the UZI CA (`ca-fingerprint`); see X509Credential with UZI server certificates.
- **Spec v1:** each Nuts node explicitly trusts issuers per credential type. Credentials such as `NutsOrganizationCredential` and `NutsEmployeeCredential` are spec v1 only.

In practice, there are the following credential issuers:

- **Governing body issuing for a specific use case**
  - In the KIK-v use case (spec v1), governed by Zorginstituut Nederland, KIK-v Beheer issues to participating organizations:
    - A credential that identifies the party as participating organization, containing a Chamber of Commerce registration number.
    - Credentials that allow a participant to perform specific SPARQL queries at another participant.
- **Use case implementors issuing with explicit trust**
  - In the eOverdracht use case (spec v1), implementing software vendors issue `NutsOrganizationCredential` for their clients. Software vendors explicitly trust each other.
- **Use case participant issuing with delegated trust**
  - In the eOverdracht use case (spec v1), participating care organizations issue a `NutsEmployeeCredential` to their active user. It is trusted when the organization has a trusted `NutsOrganizationCredential`
  - In the Huisartsinzage, PZP, and Home monitoring use cases (spec v2), parties self-issue the `X509Credential`, holding organization identity, using their CIBG UZI server certificate.

- In the LSPxNuts use cases, CIBG UZI certificates are used as backing proof for the `HealthcareProfessionalDelegationCredential`, `HealthcareProviderCredential` and `PatientEnrollmentCredential`.

Revision #6
Created 2024-04-25 17:57:59 UTC by Rein Krul
Updated 2026-10-30 15:00:41 UTC by Rein Krul