Credential Trust

Authentication on Nuts heavily depends on trusted credential issuers: any attribute, revelant 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).

In practice, there are the following credential issuers:

- **Governing body issuing for a specific use case**
  - In the KIK-v use case, governed by Zorginstituut Nederland, KIK-v Beheer issues to participating organizations:
    - A credential that identifies the party as participating (care?) 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, 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, participating care organizations issue a `NutsEmployeeCredential` to their active user. It is trusted when the organization has a trusted `NutsEmployeeCredential`
  - In the Huisartsinzage, PZP, and Home monitoring use cases, 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 #3
Created 25 April 2024 17:57:59 by Rein Krul
Updated 7 May 2026 09:14:19 by Rein Krul