AuthN using Verifiable Credentials

To successfully negotiate an OAuth2 access token, the token issuer (OAuth2 Authorization Server) will ask the client to present Verifiable Credentials. Nuts uses DIF Presentation Exchange for requesting and presenting credentials during authentication. It's used by the service-to-service (`vp_token bearer`) OAuth2 flow. It is also used by Discovery Services to restrict what can be registered on it.

Presentation Definition

The party requesting a presentation, typically during access token negotiation, provides a Presentation Definition to the credential wallet. The Presentation Definition specifies which credentials the wallet must provide. If the wallet can't fulfill the definition, access token negotiation will fail.

`NutsCareOrganization` example

Below is an example Presentation Definition specifying a `NutsOrganizationCredential`, not restricted to a specific issuer. It specifies the following:

- Only JSON-LD Verifiable Credentials are supported, which must be signed through `JsonWebSignature2020`
- No restrictions on the Verifiable Presentation format
- Credential type must be `NutsOrganizationCredential`
- `credentialSubject` of the credential must have an object `organization` with string properties `name` and `city`.

```
{
  "format": {
    "ldp_vc": {
      "proof_type": [
        "JsonWebSignature2020"
      ]
    }
  },
  "id": "pd_any_care_organization",
  "name": "Care organization",
  "purpose": "Finding a care organization for authorizing access to medical metadata",
  "input_descriptors": [
    {
      "id": "id_nuts_care_organization_cred",
      "constraints": {
```

```
      "fields": [
        {
          "path": [
            "$.type"
          ],
          "filter": {
            "type": "string",
            "const": "NutsOrganizationCredential"
          }
        },
        {
          "path": [
            "$.issuer"
          ],
          "filter": {
            "type": "string"
          }
        },
        {
          "id": "organization_name",
          "path": [
            "$.credentialSubject.organization.name"
          ],
          "filter": {
            "type": "string"
          }
        },
        {
          "id": "organization_city",
          "path": [
            "$.credentialSubject.organization.city"
          ],
          "filter": {
            "type": "string"
          }
        }
      ]
    }
  }
]
```

```
}
```

The identifiers used in the field constraints will be available in the token introspection result. The key will be the field `id` and the value will be the value in the credential that matches the `path`.

Authorizing Access Tokens through Presentation Exchange

See the DIF Presentation Exchange specification for more information.

Revision #10
Created 2024-04-25 13:54:34 UTC by Rein Krul
Updated 2026-10-28 15:10:36 UTC by Rein Krul