Proposal for EmployeeIdentity means

> This document is still in draft and is subject to change.

> Some parts are still WIP and both the English ad Dutch language is used.

In this document we propose a new *means* to identify a user. The identity is issued by the employer about the employee, hence the name `EmployeeIdentity`. The goal of this means is to reuse the information form the current session the user has within the application. This will result is a smoother user experience with the cost of less trust in the correctness of the information.

The official PR for the RFC can be found here. Check the date of the latest change to see which version is newest. Pull request on RFC002.

Uitgangspunten

Uitgangspunten bij de voorgestelde oplossing zijn als volgt:

1. Minimale impact op de ontwikkelcapaciteit van leveranciers. We weten dat er nog veel moet gebeuren voor de eOverdracht en dat de deadline snel nadert. We stellen een oplossing voor die idealiter in één dag is in te bouwen bij de leveranciers.
2. Faciliteren van een groeipad. We weten dat het gebruik van persoonlijke authenticatiemiddelen binnenkort verplicht gaat worden via wetten als de WDO en de Wegiz icm diverse NEN normen. De oplossing maakt het mogelijk voor zorginstellingen en leveranciers om eenvoudig het niveau op te hogen.
3. Voldoen aan de NEN7513. Om te kunnen voldoen aan deze norm is het belangrijk te weten welke gebruiker welke gegevens heeft ingezien. De voorgestelde oplossing voldoet aan deze eis.

Oplossingsrichting

Assurance Level eis

De zorginstelling moet zelf kunnen bepalen welke eisen ze stellen aan het vertrouwensniveua van het gebruikte middel. Daarom stellen we een nieuw veld `authenticationAssuranceLevel` voor in het `AuthorizationCredential` waarin een betrouwbaarheidsniveau van het gebruikte middel wordt opgegeven.

Het Nuts afspraken stelsel schrijft vervolgens een lijst van levels en middelen voor, bijvoorbeeld:

middel	level
EmployeeIdentity	low
Yivi(IRMA)	middle/substantial
Uzi	high

Dit level moet worden gezet per resource door de bronhouder. De opvragende partij vraagt de gebruikersidentiteit uit op het gevraagde niveau.

Voorbeeld gebruik

Onderstaand object is een voorbeeld van een credentialSubject van een `AuthorizationCredential` waar het `authenticationAssuranceLevel` veld wordt gebruikt:

```
{
  "id": "did:nuts:SjkuVHVqZndMVVJwcnUzbjhuZklhODB1M1M0LW9LcWY0WUs5S2",
  "legalBase": {
    "consentType": "explicit",
    "evidence": {
      "path": "pdf/f2aeec97-fc0d-42bf-8ca7-0548192d4231",
      "type": "application/pdf"
    }
  },
  "localParameters": {...},
  "resources": [
    {
      "path": "/DocumentReference/f2aeec97-fc0d-42bf-8ca7-0548192d4231",
      "operations": ["read"],
      "userContext": true,
      "authenticationAssuranceLevel": "low"
    }
  ],
  "purposeOfUse": "test-service",
  "subject": "urn:oid:2.16.840.1.113883.2.4.6.3:123456780"
}
```

Introductie van een nieuw EmployeeIdentity middel

Het probleem wat we op proberen te lossen is de problematiek bij implementatie, acceptatie en uitrol van persoonlijke authenticatiemiddelen. We verwachten dat zorginstellingen meer tijd nodig hebben intern beleid, ondersteuning en uitrol van deze middelen in te richten en op te tuigen. Ook is de keuze uit middelen nog beperkt waardoor deze nog niet aansluiten bij de werkprocessen van zorginstellingen. Zorginstellingen geven aan terug te willen vallen op bestaande afspraken onderling en elkaar daarin te vertrouwen met het identificeren van medewerkers. Daarom introduceren we het `EmployeeIdentity` middel. Dit middel is van niveau `low` en gebruikt de identiteit van de ingelogde gebruiker.

Dit middel is een drop-in replacement voor het Yivi(IRMA) middel.

Create signing session

Current payload for the IRMA means:

```
POST /internal/auth/v1/signature/session
{
  "means": "irma",
  "payload": "EN:PractitionerLogin:v3 I hereby declare to act on behalf of CareBears located in CareTown. This declaration is valid from Monday, 2 January 2006 15:04:05 until Monday, 2 January 2006 17:04:05."
}
```

Proposed payload for the EmployeeIdentity means:

```
POST /internal/auth/v1/signature/session
{
  "means": "employeeIdentity",
  "params": {
    "employer":"did:123",
    "emplopyee": {
      "identifier": "481",
      "roleName": "Verpleegkundige niveau 2",
      "initials": "J",
      "familyName": "van Dijk",
      "email": "j.vandijk@example.com"
    }
  },
  "payload": "EN:PractitionerLogin:v3 I hereby declare to act on behalf of CareBears located in CareTown. This declaration is valid from Monday, 2 January 2006 15:04:05 until Monday, 2 January 2006 17:04:05."
}
```

Response:

IRMA:

```
{
  "sessionID": "123",
  "sessionPtr": {QRCode},
  "means": "irma"
}
```

The frontend renders the contents of the `sessionPtr` as a QRCode.

EmployeeIdentity:

```
{
  "sessionID": "123",
  "sessionPtr": { "url":"nuts.example.com/public/auth/employeeID/123" },
  "means": "irma"
}
```

De frontend uses the `url` from the `sessionPtr` object to open a new browser window or render the page in a iframe.

Polling for the session status

IRMA en EmployeeIdentity:

`GET /internal/auth/v1/signature/session/{sessionID}`

Pending, as long as the user is signing the contract:

```
{
    "status": "pending"
}
```

Completed:

```
{
  "status": "completed",
  "verifiablePresentation": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
```

```
      "https://nuts.nl/credentials/v1",
      "http://schema.org/",
      "https://w3c-ccg.github.io/lds-jws2020/contexts/lds-jws2020-v1.json"
    ],
    "type": ["VerifiablePresentation", "NutsSelfSignedPresentation"],
    "verifiableCredential": [
      {
      "issuer": "did:nuts:careOrg",
        "type": ["VerifiableCredential", "NutsEmployeeCredential"],
        "expirationDate": "2023-04-03T20:34:17.687862+01:00",
        "credentialSubject": {
          "type":"Organization",
          "id":"did:nuts:123456789",
          "member":{
            "type":"EmployeeRole",
            "identifier": "481",
            "roleName": "Verpleegkundige niveau 2",
            "member": {
              "type": "Person",
              "initials": "J",
              "familyName": "van Dijk",
              "email": "j.vandijk@example.com"
            }
          }
        }],
      "proof": {
        "type": "JsonWebSignature2020",
        "verificationMethod": "did:nuts:123456789#key-1",
        "created": "2023-04-03T16:34:17.687862+01:00",
        "jws":
"eyJhbGciOiJFUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..hKcboC8m6YnZPi6ReJAYs0J0Ztn5nxcx2EavoXdtr
kWxmE1JZmImW89_8IIgjvfI8XtGeDlEnGywAuY2u7y9Bw"
      }
    },
    "proof": {
      "challenge": "LOGIN CONTRACT",
      "type": "JsonWebSignature2020",
      "verificationMethod": "did:nuts:123456789#key-1",
      "created": "2023-04-03T16:34:17.687862+01:00",
      "jws":
```

"eyJhbGciOiJFUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..hKcboC8m6YnZPi6ReJAYs0J0Ztn5nxcx2EavoXdtrkWxmE1JZmImW89_8IIgjvfI8XtGeDlEnGywAuY2u7y9Bw"
  }
 }
}

Usage of the identity token

The usage of the returned identity is the same for IRMA and EmployeeIdentity: the value of the `verifiablePresentation` field is base64 encoded and added to the access token request in the `usi` field.

TODO

- **Remove evidence (done)**
  Evidence in the presentation does not provide enough evidence and might even expose internal IPs.
- **Add new types to the Nuts JSON-LD context**
  Add both NutsEmployeeCredential and NutsSelfIssuedPresentation to the JSON-LD context.
- **Create RFC for NutsSelfSignedPresentation**
  This presentation hints to a verifier that the containing credential(s) have the same subject and issuer.

(Open) Issues

- **Fix backwards compatibility of JSON-LD context**
  How to make sure signatures on the new NutsAuthorizationCredential are valid when the new field `assurenceLevel` is added but not all nodes are updated and have the new context?
- **Proof of ownership for the credential**
  How to validate the proof signature of presentation? Normally the holder == subject and signs the presentation. Now the presentation is signed by the issuer. Solution: add the NutsOrgCredential to the presentation, add extra `NutsSelfIssuedPresentation` type to the presentation. e.g. `trusted(vendor)? && Verify(vendor -> org -> employeeRole)`
- **Make sure that the form can be embedded inside an iframe**
  Do research for how to configure CORS. Do we need to provide css for usage with and without iframe?

Revision #6
Created 5 April 2023 07:51:02 by Steven van der Vegt
Updated 12 April 2023 11:00:48 by Wout Slakhorst