Nuts-application eOverdracht 2.0

Introduction

This articles specifies version 2 of the Nuts-application-specification "eOverdracht" of which version 1.0 is published on: Leveranciersspecificatie. This article describes the necessary changes to version 1.0 to make eOverdracht work using `did:web`, without relying on the use of `did:nuts` and/or `NutsAuthorizationCredentials`.

Attribute based authorization

Given new insights into authorizations, the `NutsAuthorizationCredentials` are no longer used as notification or authorization method. In the new approach Attribute Based Access Control (ABAC) moves away from authorizations in (verifiable) credentials to using credentials merely for providing attributes. Verifiable Credentials (in Nuts) are limited to providing attributes. In the previous version, authorization decisions were made based on the contents of `NutsAuthorizationCredentials`, with the ABAC approach the Task will be used for authorizations.

1. With the ABAC approach to authorization, decisions are made based on the contents of FHIR `Tasks` in combination with the identity of the requester.
2. The specific resources that may be accessed are known in advance, since they are listed in the FHIR `Task`.
3. Instead of issuing an `AuthorizationCredential` to a DID, the `sender` maps the URA of the receiver to the resources internally using the `owner` element in the FHIR `Task`.

X509Credential for organization identification and authentication

The attribute based authorization needs a new kind of credential.

1. With the arrival of `X509Credential` it has become possible to use an trusted source of trust to the eOverdracht authentication framework, the need for a `NutsOrganizationCredential` has become less relevant.
2. The `X509Credential` is used to identify and authenticate the `sender` and `receiver` healthcare organizations.
3. All participants must get a UZI server certificate. The URA number will be the functional identifier and the organisation name (`O`) from the server certificate will be used as name to search on.
4. Vendors will no longer need to trust specific DIDs.

Discovery

With the departure from `did:nuts`, the newly created discovery service in `did:web` needs to be leveraged to be able to discover organizations. The id of the discovery service will be `eoverdracht2025` and will require a `X509Credential` to be indexed for discovery.

The following registration parameters are required:

- `roles`: an array of `['sender','receiver']`. This tells others for which roles the registration is.
- `fhir`: the FHIR endpoint URL
- `notification`: The notification URL if the registration has the `receiver` role.

User identification

Version 2.0 makes use of the `NutsEmployeeCredential` for authenticating the user. Authentication based on `YIVI` / `IRMA` is no longer used.

Changes to version 1.0 per section

This chapter describes the necessary changes to version 1.0 of the specification, per section.

4.1.1

The current Task describes that the Task is used to track the progress of the hand-off. This is correct but the Task will also be used as authorization mechanism. Add text: Besided the Task being used to track progress, it will be used to specify which organization (actor) has acccess to handoff data of which patient.

4.1.2

does this need changes? do we need separate eoverdracht-services for did:web-implementations?

4.1.3

can be changed to R5 notification backport and server-managed-subscriptions. But it is not necessary to change this to become did:web-compatible. proposal: keep unchanged.

5.3 retrieve hand off message

Sequence diagram

Current sequence diagram should be replaced by. insert new plantuml here.

5.3.1 Register authorization

The current text describes the registration and distribution of a NutsAuthorizationCredential. This text should be deleted.

5.3.2 Notification

Loopup notification endpoint

Is a change necessary?

5.3.3

no changes?

5.3.4 Authentication

Person authentication

The current text describes user authentication based on IRMA. This text should be replaced by user authentication based on `NutsEmployeeCredential`

5.3.5 retrieve hand off message

do we need a separate endpoint for did:web fhir-requests?

request access token

NutsAuthorizationCredential is not supported Replace by ... VP with URA of actor organization is mandatory VP with attributes of end user is mandatory

apply authorization by custodian/ data holder

Do not use NutsAuthorizationCredential but check

1. is there a valid Task
2. is the Task.state "active"/"x"/"y"
3. is the URA in the VP present in the Task.owner-element? refer to Rego-code (section 6.2)

5.3.6

Delete use of NutsAuthzCredentials

6 access policy

Describe two new policies that should be used in did:web-implementations:

eOverdracht-receiver-did-web policy

Like 6.1 but ...

eOverdracht-sender-did-web policy

non-PID resources

Like 6.2.1 but....

PID resources

Like 6.2.2 but ...

6.3

Delete use of AuthzCredentials.

where to put?

Organization authentication

x509 must be used to authenticate healthcare organizations based on URA number/ UZI server certificates.

Wouts notes (have to be placed somewhere):

Discovery

eOverdracht participants are currently participants if they:

- have published an `NutsOrganizationCredential`, and;
- they registered `eOverdracht-sender` and/or `eOverdracht-receiver` services in their DID Document. This will be replaced with an entry in the discovery service for eOverdracht. The id will be `eoverdracht2025`. The service definition for the discovery service will require a `X509Credential` linked to the public key from UZI and a requirement on `SAN` and `O` (and others). When registering, the following registration parameters are required (can be added to service definition):

- `roles`: an array of `['sender','receiver']`. This tells others for which roles the registration is.
- `fhir`: the FHIR endpoint URL
- `notification`: The notification URL if the registration has the `receiver` role. Note: the authServerURL is added automatically. Services in DID Documents are no longer needed. Publishing of the `NutsOrganizationCredential` is no longer needed.

PresentationDefinition

The `X509Credential` must be set in the `eoverdracht2025` presentation definition mapping. This is probably the same as the part in the service definition.

Access token

The V2 request-service-access-token API must be used to request the access token. The `authorizationServer` param is retrieved when searching the discovery service. The `scope` must be `eoverdracht2025`. A `NutsEmployeeCredential` must be added when retrieving medical data as receiver. (similar to the `userContext` concept in auth creds). The `X509Credential` must not be added in the call but must exist in the wallet of the organisation using the holder load API.

Resource request

The access token from the previous step is added as bearer token. The notification task can be posted to the `notification` endpoint which is found by the discovery service search. Resources can be retrieved from the `fhir` endpoint appended with the specific resource path from the `task.input` field.

Authorization

The resource server will forward the bearer token to the node introspection endpoint. This will return the required fields from the presentation definition as values. This will give the URA number. The authoriser can check its internal mapping if the requested resource may be accessed by the given URA.

did:web

After implementation and activation of the above, did:web can be introduced. If DIDs no longer issue credentials (NutsOrg and NutsAuth creds) then clustering can be enabled.

Revision #8
Created 2025-03-25 14:40:56 UTC by Jorrit Spee
Updated 2025-03-31 11:22:28 UTC by Roland Groen