Requesting Access

To access APIs secured through Nuts, callers need an access token issued by the OAuth2 Authorization Server of the API owner. This page describes how to acquire an access token.

Requesting Service Access Token

This section describes which value(s) need to be specified in the service access token request.

- In the request URL:
  - `subjectID`: the ID of the local requester, which was provided by the Nuts node when the subject and its DIDs was created.
- In the request body:
  - `authorization_server`: the OAuth2 issuer URL of the party that grants access, found in the service discovery search result.
  - `scope`: specifies what resources the access token will give access to. This is specified by the use case.
  - `credentials` (optional): one or more credentials to provide to the authorization server that are not in the requester's wallet. This is typically used to provide an `NutsEmployeeCredential` to the authorization server. See the section below for how to provide this.
  - `token_type` (optional): by default, tokens are of type DPoP that mitigate token theft. Alternatively, the `Bearer` token type can be specified, but you'll be more vulnerable to MITM attacks.

Example

```
POST http://<nuts private API>/internal/v2/auth/<subjectID>/request-service-access-token
Content-Type: application/json


{
  "authorization_server": "https://example.com/oauth2/hospital_x",
  "scope": "eOverdracht-sender"
}
```

Providing additional credentials

The service access token request allows you to supply credentials to the request, that are not in the subject's wallet but required for authentication. For instance, an `EmployeeCredential` that

contains information about the current logged-in user for logging purposes. These credential don't need to be signed: in that case they will be "self-attested" (e.g., the `EmployeeCredential`); the Verifiable Presentation's signature will provide authenticity.

Example

The example below shows an example access token request with an `EmployeeCredential`.

```
POST http://<nuts private API>/internal/v2/auth/<subjectID>/request-service-access-token
Content-Type: application/json

{
  "authorization_server": "https://example.com/oauth2/hospital_x",
  "scope": "eOverdracht-sender",
  "credentials": [
     {
       "@context": [
         "https://www.w3.org/2018/credentials/v1",
         "https://nuts.nl/credentials/v1"
       ],
       "type": ["VerifiableCredential", "NutsEmployeeCredential"],
       "credentialSubject": {
         "name": "John Doe",
         "roleName": "Nurse",
         "identifier": "123456"
       }
     }
   ]
}
```

Revision #10
Created 10 September 2024 09:32:54 by Rein Krul
Updated 23 September 2024 07:21:32 by Rein Krul