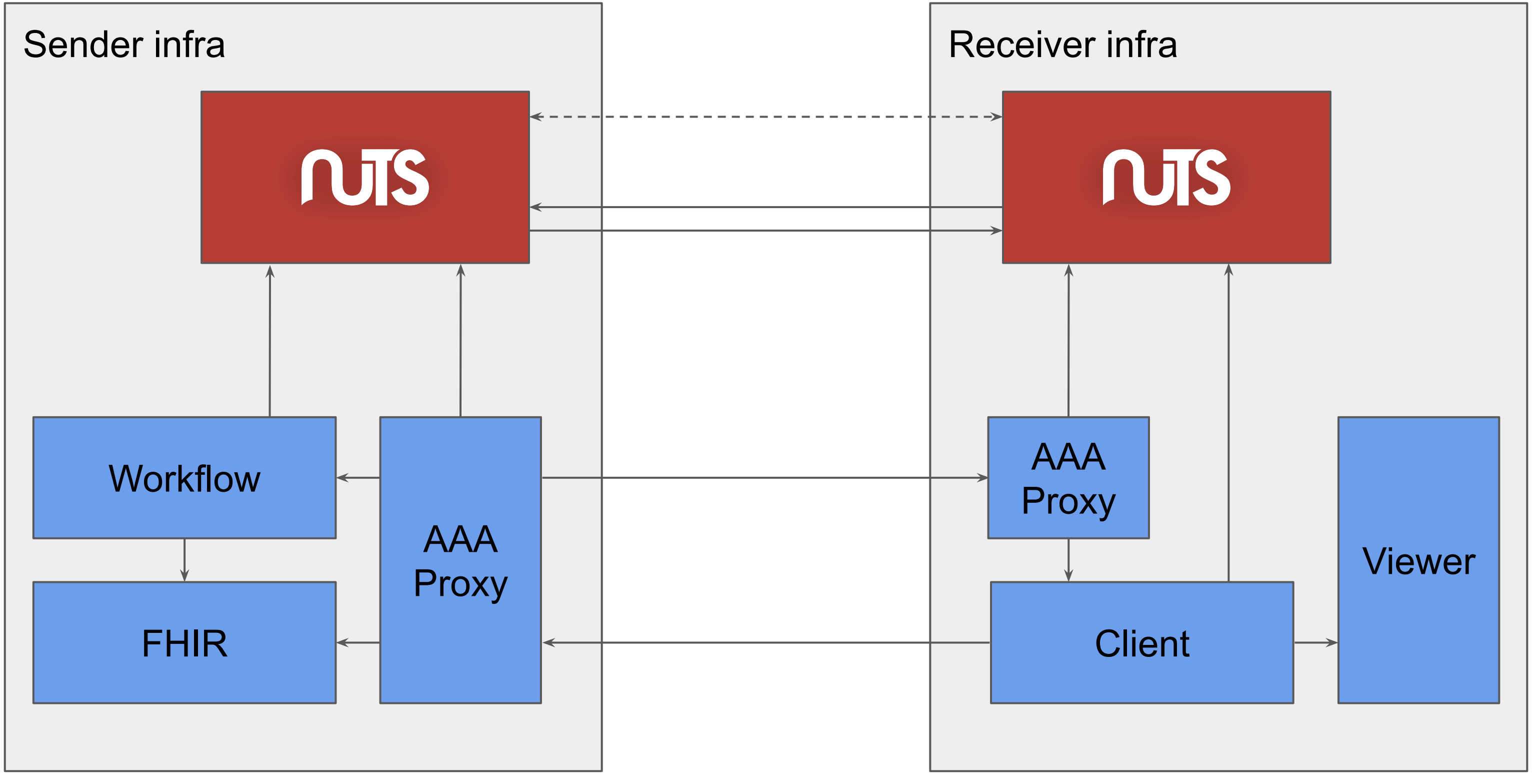
Goal/Agenda today

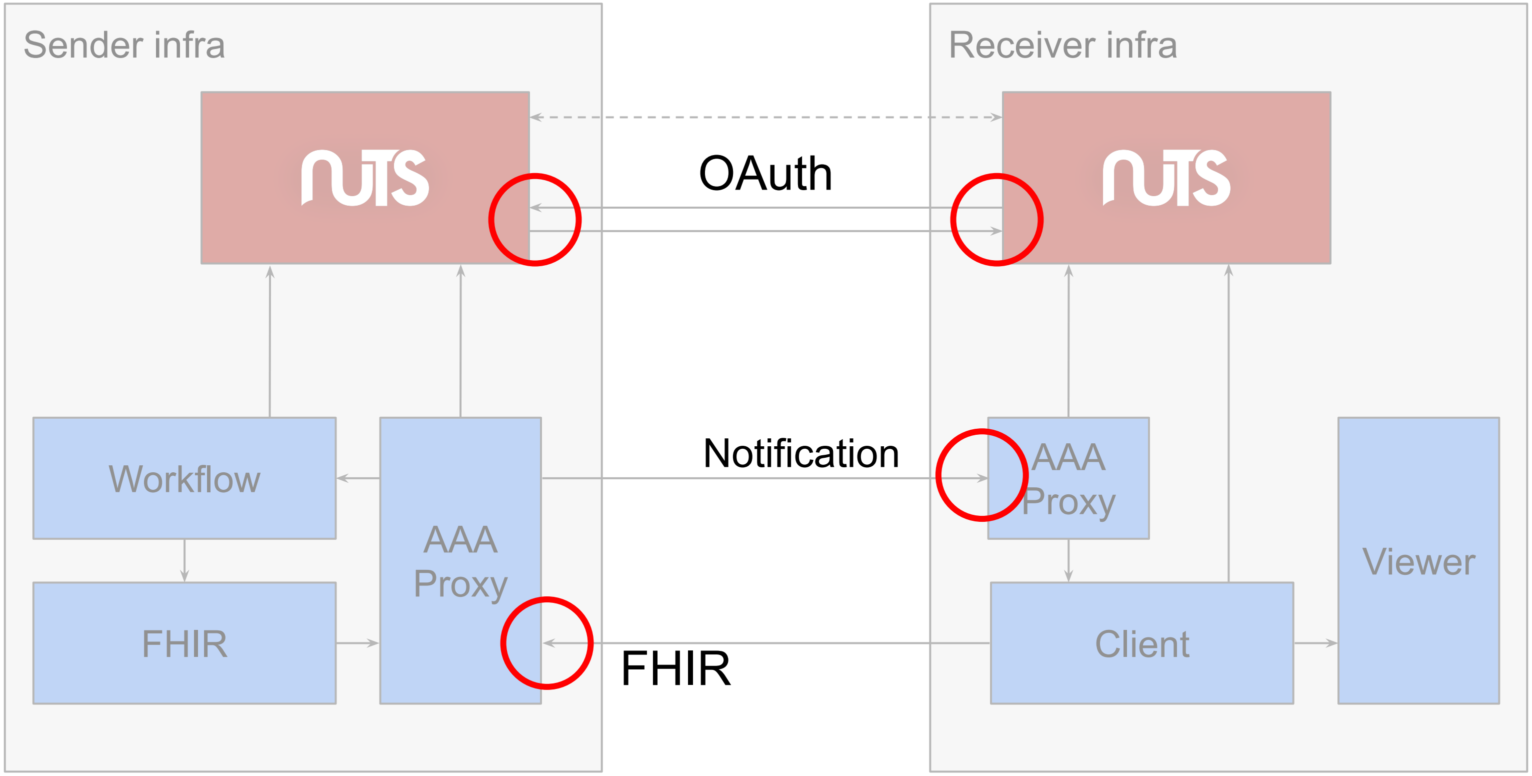
- API security
- Using authorization credentials
- Authenticating users

https://github.com/nuts-foundation/nuts-workshops
https://nuts-node.readthedocs.io/en/latest/
https://nuts-foundation.gitbook.io/drafts/
https://nuts-foundation.gitbook.io/bolts/eoverdracht/leveranciersspecificatie

Architecture



Service endpoints



Sender service

- Type: **`eOverdracht-sender`**
- **`oauth`** member pointing to authorization server endpoint
- **`fhir`** member pointing to fhir endpoint

```
{
  "id": "did:nuts:gwng...3SH#F1Dsgwngfdg3SH6TpDv0Ta1aOE",
  "type": "eOverdracht-sender",
  "serviceEndpoint": {
    "oauth": "http://192.168.1.xx:1323/n2n/auth/v1/accesstoken",
    "fhir": "http://192.168.1.xx:1304/fhir"
  }
}
```

https://nuts-foundation.gitbook.io/bolts/eoverdracht/leveranciersspecificatie#4-1-2-organisatie-endpoint-discovery

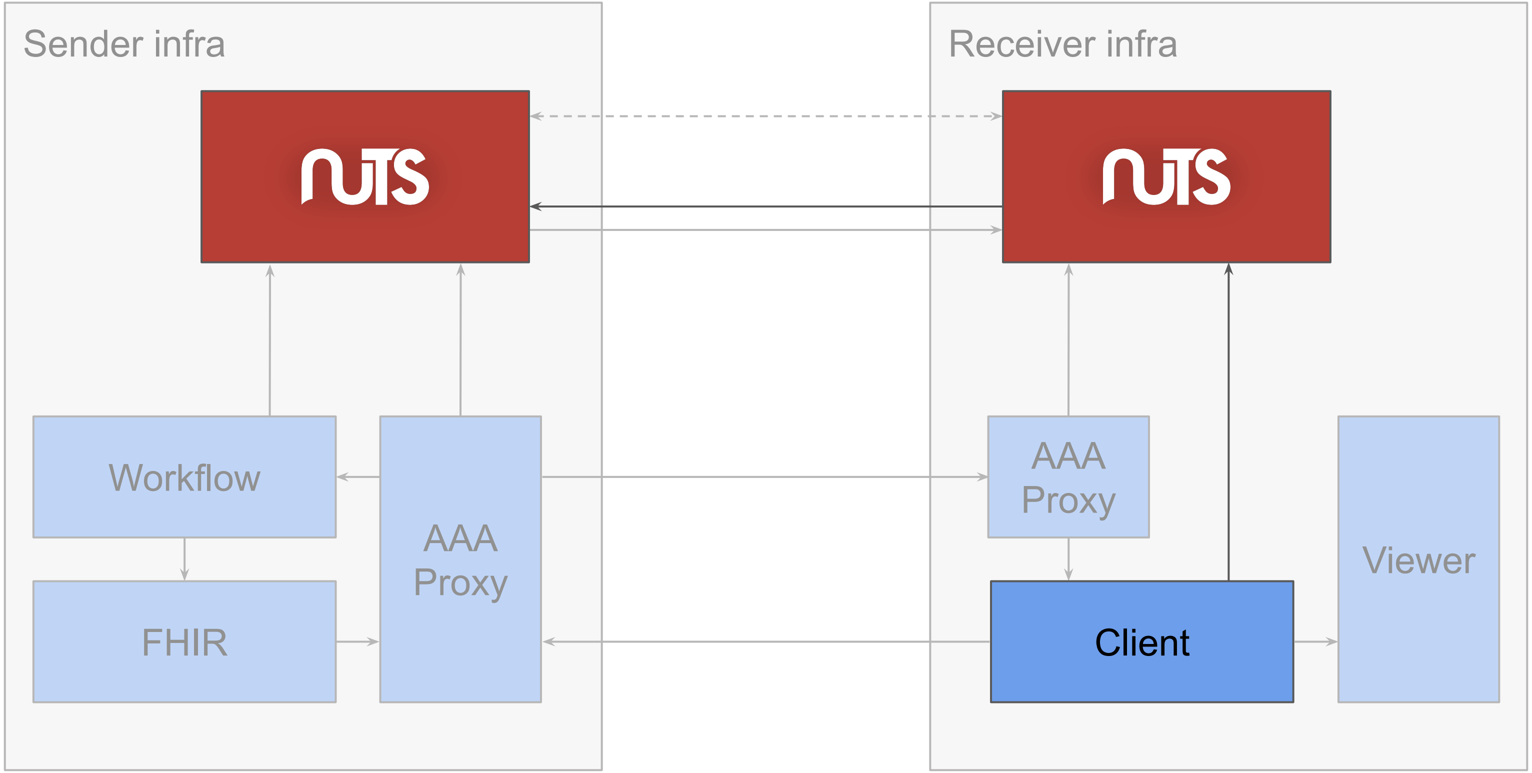
Receiver service

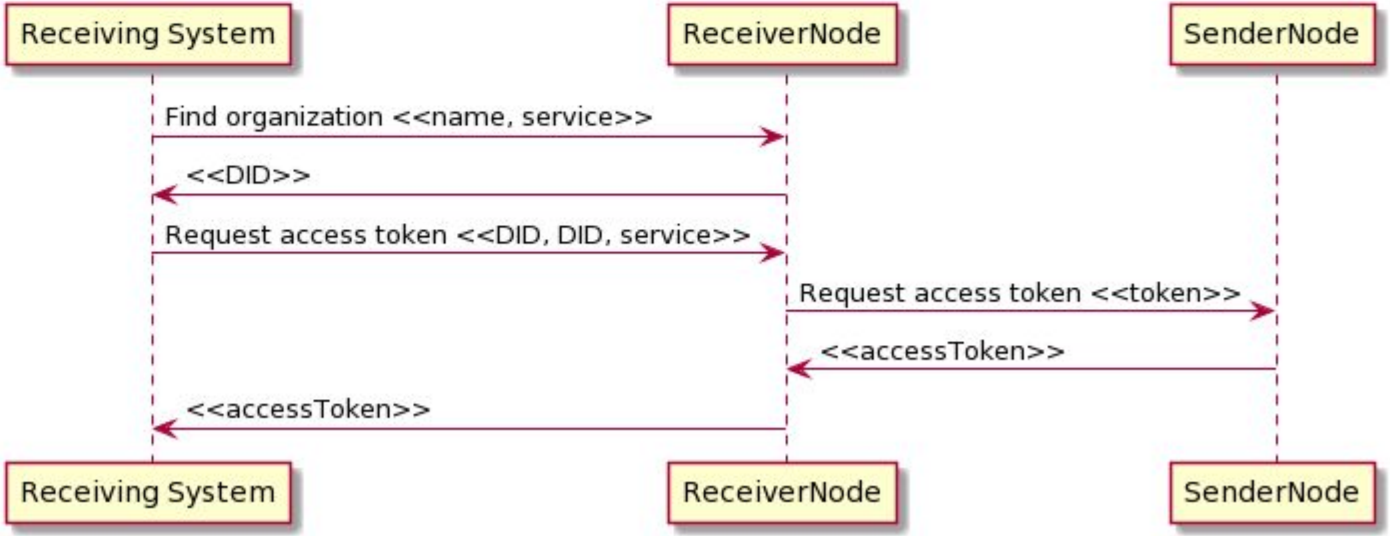
- Type: **`eOverdracht-receiver`**
- **`oauth`** member pointing to authorization server endpoint
- **`notification`** member pointing to notification endpoint

```
{
  "id": "did:nuts:gwng...3SH#F1Dsgwngfdg3SH6TpDv0Ta1aOE",
  "type": "eOverdracht-receiver",
  "serviceEndpoint": {
    "oauth": "http://192.168.1.xx:1323/n2n/auth/v1/accesstoken",
    "notification": "192.168.1.xx:1304/web/external/transfer/notify"
  }
}
```

https://nuts-foundation.gitbook.io/bolts/eoverdracht/leveranciersspecificatie#4-1-2-organisatie-endpoint-discovery

Security: request access token





Receiving System

ReceiverNode

SenderNode

Find organization <<name, service>>

<<DID>>

Request access token <<DID, DID, service>>

Request access token <<token>>

<<accessToken>>

<<accessToken>>

Receiving System

ReceiverNode

SenderNode

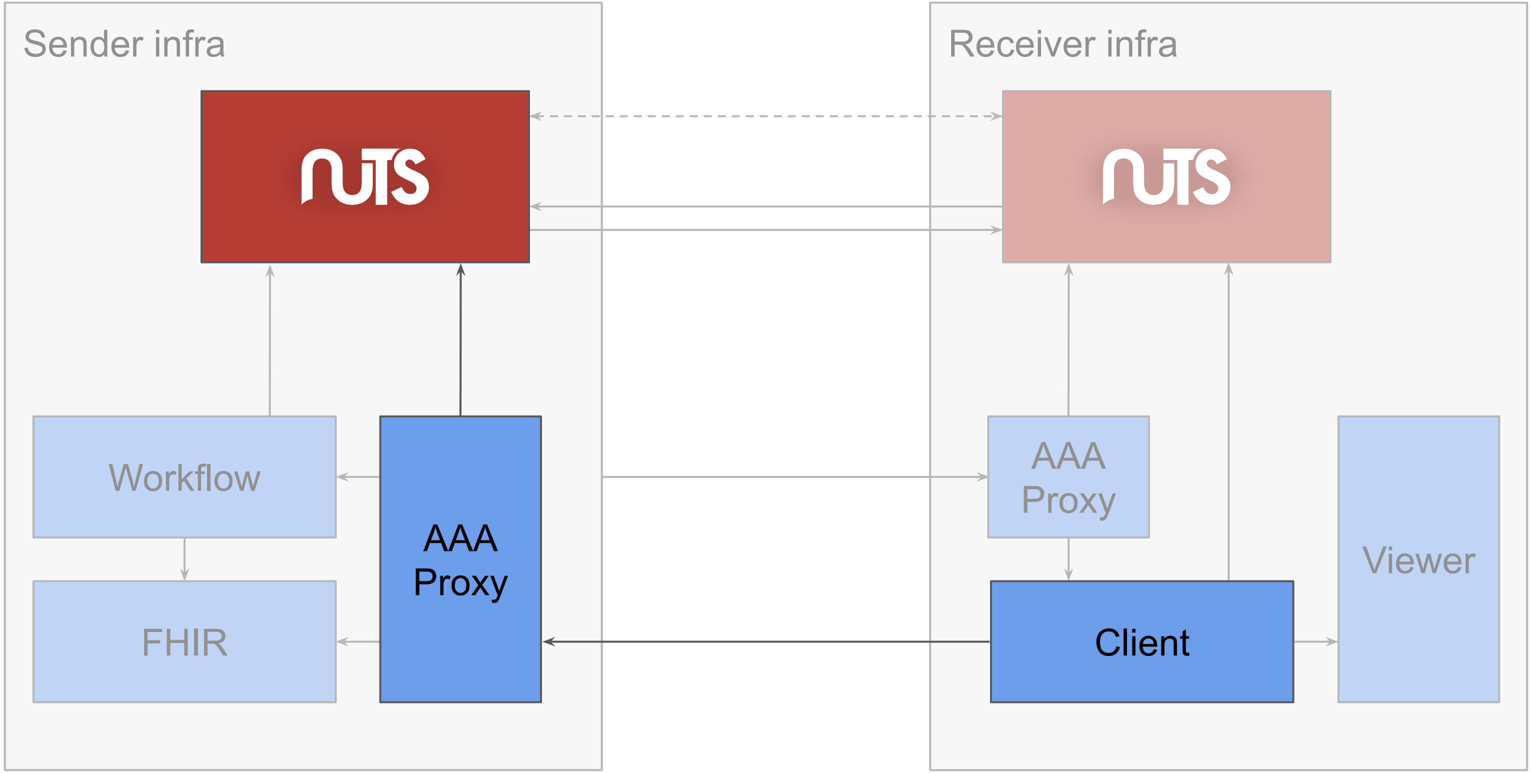
Requests

```
GET http://localhost:1323/internal/didman/v1/search/organizations
POST http://localhost:1323/internal/auth/v1/request-access-token
```

```
{
  "authorizer": "{DID}",
  "requester": "{DID}",
  "service": "eOverdracht-sender"
}
```

https://nuts-node.readthedocs.io/en/latest/pages/api.html

Security: check access token



Requests

```
POST http://localhost:1323/internal/auth/v1/accesstoken/introspect
```

```
{"token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJha...SHMynYSA"}
```

```
{
  "active": true,
  "service": "eOverdracht-sender",
  "iss": "did:nuts:sender",
  "sub": "did:nuts:receiver",
  "aud": "http://{demo_IP+port}",
  "exp": 0,
  "iat": 0,
  "name": "Willeke de Bruijn",
  "family_name": "Bruijn",
  "prefix": "de",
  "given_name": "Willeke",
  "email": "w.debruijn@example.org"
}
```

GO NUTS!

NutsAuthorizationCredential

https://nuts-foundation.gitbook.io/drafts/rfc/rfc014-authorization-credential

```
{
    "@context": ["https://www.w3.org/2018/credentials/v1","https://nuts.nl/credentials/v1"],
    "id":"did:nuts:C46nMckdjGK3RMwFf6o3wZ522MCUBeHiDevMXn2mFruT#5b56d0da-4476-41f4-a0fd-7a79d12eb73b",
    "type": ["NutsAuthorizationCredential", "VerifiableCredential"],
    "issuanceDate": "2021-09-07T12:47:38.2932788Z",
    "issuer": "did:nuts:C46nMckdjGK3RMwFf6o3wZ522MCUBeHiDevMXn2mFruT",
    "credentialSubject": {
        "id": "did:nuts:42wTGxWYd3XdnR4mGSqLXypAxdwG2duNxYJS82MaGn2w",
        "legalBase": {
            "consentType": "implied",
            "evidence": null
        },
        "purposeOfUse": "eOverdracht-sender",
        "resources": [
            {
                "operations": [
                    "read",
                    "update"
                ],
                "path": "/Task/872765d9-4304-48a7-93b8-032b6b637833",
                "userContext": false
            }
        ],
        "subject": null
    },
    "proof": {...}
```

Adding a NutsAuthorizationCredential

```
POST http://localhost:1323/internal/vcr/v1/vc
```

```
{
  "type": "NutsAuthorizationCredential",
  "issuer": "did:nuts:B8PUHs2AUHbFF1xLLK4eZjgErEcMXHxs68FteY7NDtCY",
  "expirationDate": "2012-01-02T12:00:00Z",
  "credentialSubject": {}
}
```

https://nuts-node.readthedocs.io/en/latest/pages/api.html

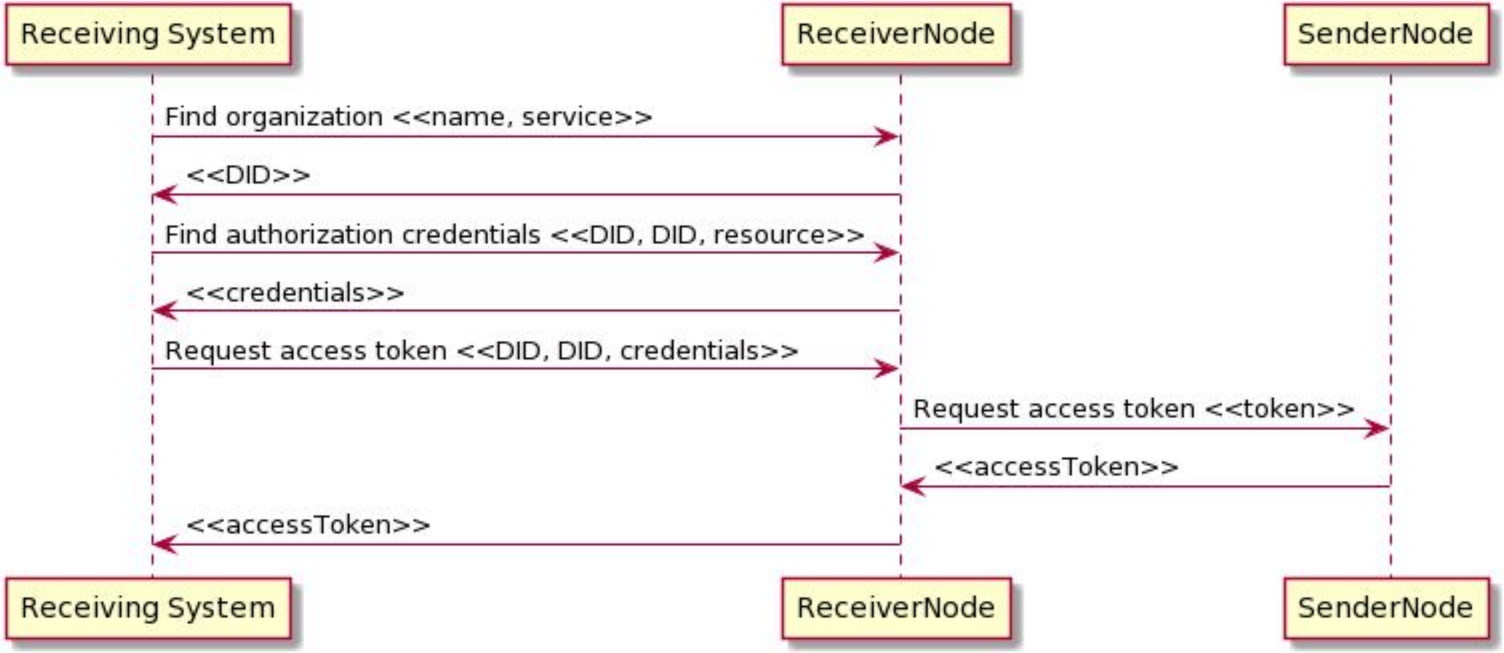
Search a NutsAuthorizationCredential

```
POST http://localhost:1323/internal/vcr/v1/authorization?untrusted=true
```

```
{
  "credentialSubject.id": "did:nuts:B8PUHs2AUHbF...ZjgErEcMXHxs68FteY7NDtCY",
  "credentialSubject.purposeOfUse": "eOverdracht-sender",
  "credentialSubject.resources.#.path": "/Task/872765d9-4304-48a7-93b8-032b6b637833"
}
```

https://nuts-node.readthedocs.io/en/latest/pages/api.html

Security: request access token



Receiving System

ReceiverNode

SenderNode

Find organization <<name, service>>

<<DID>>

Find authorization credentials <<DID, DID, resource>>

<<credentials>>

Request access token <<DID, DID, credentials>>

Request access token <<token>>

<<accessToken>>

<<accessToken>>

Receiving System

ReceiverNode

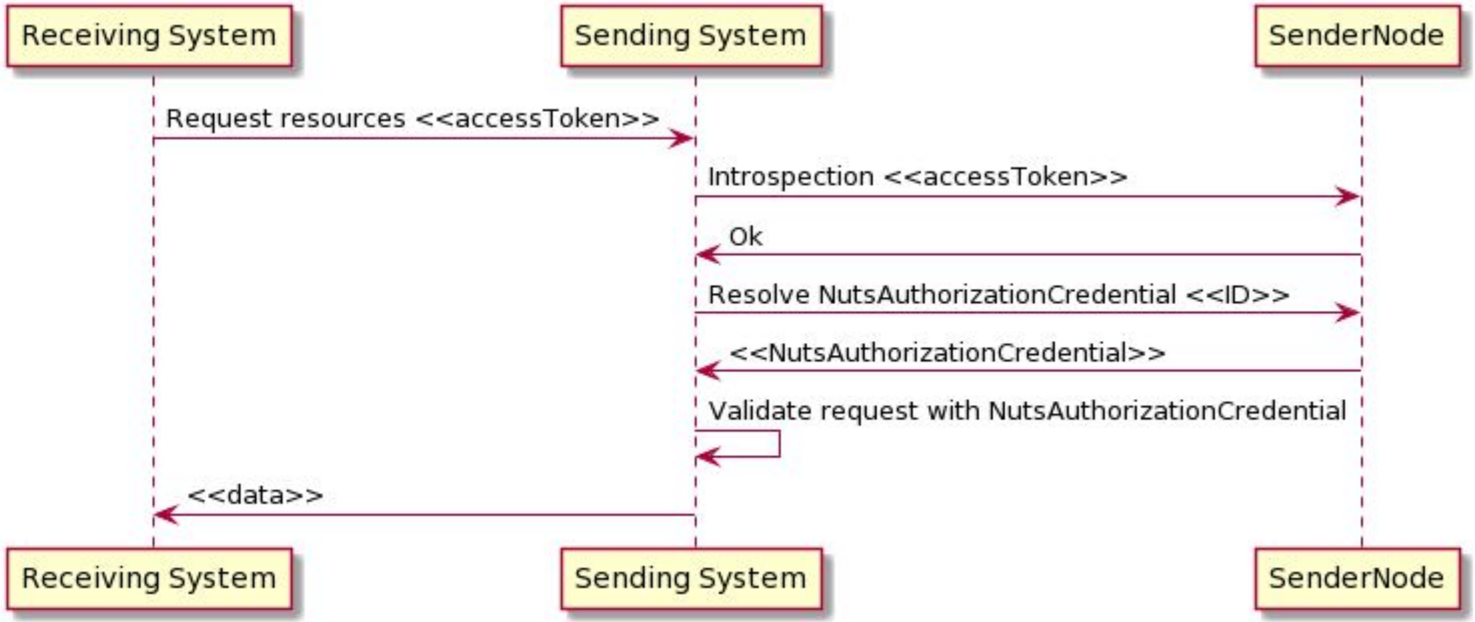
SenderNode

Requests

```
POST http://localhost:1323/internal/auth/v1/request-access-token
```

```
{
  "authorizer": "{DID}",
  "requester": "{DID}",
  "service": "eOverdracht-sender"
  "credentials": [
    {
      "@context": ["..."],
      "Id": "did:nuts:C46nMd...FruT#5b56d0da-4476-41f4-a0fd-7a79d12eb73b",
      "type": ["NutsAuthorizationCredential", "VerifiableCredential"],
      "issuer": "did:nuts:B8PUHs2AUHbFF1xLLK4eZjgErEcMXHxs68FteY7NDtCY",
      "issuanceDate": "2012-01-02T12:00:00Z",
      "expirationDate": "2012-01-02T12:00:00Z",
      "credentialSubject": {},
      "proof": {}
    }
  ]
}
```

Validation



Receiving System

Sending System

SenderNode

Request resources <<accessToken>>

Introspection <<accessToken>>

Ok

Resolve NutsAuthorizationCredential <<ID>>

<<NutsAuthorizationCredential>>

Validate request with NutsAuthorizationCredential

<<data>>

Receiving System

Sending System

SenderNode

Requests

```
POST http://localhost:1323/internal/auth/v1/accesstoken/introspect
```

```
token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJha...SHMynYSA
```

```
{
  "active": true,
  "service": "eOverdracht-sender",
  "iss": "did:nuts:sender",
  "sub": "did:nuts:receiver",
  "aud": "http://{demo_IP+port}",
  "exp": 0,
  "iat": 0,
  "name": "Willeke de Bruijn",
  "family_name": "Bruijn",
  "prefix": "de",
  "given_name": "Willeke",
  "email": "w.debruijn@example.org"
  "vcs": ["did:nuts:C46nMd...FruT#5b56d0da-4476-41f4-a0fd-7a79d12eb73b"],
}
```

Resolving VCs

```
GET http://localhost:1323/internal/vcr/v1/vc/{id}
```

```
{
  "currentStatus": "trusted",
  "verifiableCredential": {
    ...
  }
}
```

currentStatus can be “trusted”, “untrusted” or “revoked”.
Resolving a credential not valid at the given time returns an error. “As if it didn’t exist”

https://nuts-node.readthedocs.io/en/latest/pages/api.html

Authentication

```json
{
    "@context": ["https://www.w3.org/2018/credentials/v1","https://nuts.nl/credentials/v1"],
    "id":"did:nuts:C46nMckdjGK3RMwFf6o3wZ522MCUBeHiDevMXn2mFruT#5b56d0da-4476-41f4-a0fd-7a79d12eb73b",
    "type": ["NutsAuthorizationCredential", "VerifiableCredential"],
    "issuanceDate": "2021-09-07T12:47:38.2932788Z",
    "issuer": "did:nuts:C46nMckdjGK3RMwFf6o3wZ522MCUBeHiDevMXn2mFruT",
    "credentialSubject": {
        "id": "did:nuts:42wTGxWYd3XdnR4mGSqLXypAxdwG2duNxYJS82MaGn2w",
        "legalBase": {
            "consentType": "implied",
            "evidence": null
        },
        "purposeOfUse": "eOverdracht-sender",
        "resources": [
            {
                "operations": [
                    "read",
                    "update"
                ],
                "path": "/Task/872765d9-4304-48a7-93b8-032b6b637833",
                "userContext": false
            }
        ],
        "subject": null
    },
    "proof": {...}
```

Request an access token

```
POST http://localhost:1323/internal/auth/v1/request-access-token
```

```
{
  "authorizer": "{DID}",
  "requester": "{DID}",
  "service": "eOverdracht-sender"
  "credentials": [...],
  "identity": "...",
}
```

https://nuts-node.readthedocs.io/en/latest/pages/api.html

Obtaining the user identity (1)

```
PUT http://localhost:1323/internal/auth/v1/contract/drawup
```

```
{
     Language:    "NL",
     LegalEntity: "did:nuts:alkn834...alici871",
     Type:        "BehandelaarLogin",
     ValidFrom:   "2021-09-27T12:00:00Z",
     Version:     "v3",
}
```

```
{
  "message": "NL:BehandelaarLogin:v3 Hierbij verklaar ik te handelen in naam van CareBears
te CareTown. Deze verklaring is geldig van 2021-09-27T12:00:00 tot 2021-09-27T13:00:00.",
  "type": "BehandelaarLogin",
  "language": "NL",
  "version": "v1"
}
```

https://nuts-node.readthedocs.io/en/latest/pages/api.html

Obtaining the user identity (2)

```
POST http://localhost:1323/internal/auth/v1/signature/session
```

```
{
  "means": "dummy",
  "payload": "NL:BehandelaarLogin:v3 Hierbij verklaar ik te handelen in naam van CareBears te CareTown. Deze verklaring is geldig van 2021-09-27T12:00:00 tot 2021-09-27T13:00:00."
}
```

```
{
  "sessionID": "lkasck485nlackhnas",
  "sessionPtr": {},
  "means": "dummy"
}
```

https://nuts-node.readthedocs.io/en/latest/pages/api.html

Obtaining the user identity (3)

```
GET http://localhost:1323/internal/auth/v1/signature/session/{sessionID}
```

```
{
  "status": "completed",
  "verifiablePresentation": {...}
}
```

The base64 representation of the *verifiablePresentation* is to be used in the access token request.
Using IRMA instead of dummy is described here:
https://nuts-node.readthedocs.io/en/latest/pages/getting-started/5-irma-contract.html
UZI means can also be used. (manual pending)

https://nuts-node.readthedocs.io/en/latest/pages/api.html

Final note

All flows are described in compact manuals. You can find them here: https://github.com/nuts-foundation/nuts-workshops/mini-manuals

Hacking: Task/Composition
Hacking: User login

GO NUTS!