

Make the FHIR call

With an access token, you can query the other care organization's FHIR API (or other data API).

The token is either a DPOP token (the default) or a Bearer token, depending on `token_type` in your token request. DPOP is optional, but more secure: every request also needs a DPOP header, which proves the request comes from you, the party the token was issued to. A stolen DPOP token is useless without your node's key. Your Nuts node creates the DPOP header for you.

Before you start

- You have an access token and its `dpop_kid` (see "Request an access token").
- You have the other care organization's API endpoint, from its `registrationParameters` (see "Find care organizations and their endpoints").
- Your client can connect to the other party's API. Data endpoints are protected with mTLS (see "Endpoints and TLS certificates").

1. Create the DPOP header (DPOP tokens only)

Create a new DPOP header for **every** request. It's only valid for one HTTP method and URL, and can only be used once.

```
POST <internal Nuts interface>/internal/auth/v2/dpop/<dpop_kid, URL-encoded>
```

```
Content-Type: application/json
```

```
{
  "htm": "<HTTP method>",
  "htu": "<URL of the request>",
  "token": "<access token>"
}
```

Field	Value
<code><dpop_kid></code> (in the URL)	<code>dpop_kid</code> from the token response, URL-encoded once, e.g. <code>#</code> becomes <code>%23</code>
<code>htm</code>	The HTTP method of the request you're about to make, e.g. <code>GET</code>
<code>htu</code>	The URL of the request you're about to make. Query parameters are ignored.
<code>token</code>	The access token

The response:

```
{
  "dpop": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpzZW50b3Rhd0In0..."
}
```

2. Make the request

Send the access token in the `Authorization` header with the type `DPoP`, and the DPoP header in `DPoP`:

```
<HTTP method> <URL of the request>
Authorization: DPoP <access token>
DPoP: <dpop from step 1>
```

For a Bearer token, skip step 1 and send `Authorization: Bearer <access token>`.

Errors

Response from the other party	What to do
401 Unauthorized	The token expired, or the DPoP header doesn't match the request. Check <code>htm</code> and <code>htu</code> . If the token expired, request a new one. If it hasn't expired, the other party may have lost it: request a new token with the header <code>Cache-Control: no-cache</code> , which skips your node's token cache.
403 Forbidden	The other party doesn't allow this query, e.g. no legal basis such as consent. Check the use case's rules.

360-graden-clientbeeld

Use `fhirR4BaseURL` or `fhirStu3BaseURL` from the search result, depending on which FHIR version the other party offers. The examples below use R4, with base URL `https://fhir.other.example/r4`.

1. Get the CapabilityStatement. It says which queries the other party supports. It doesn't need an access token, and you need it before any query other than Patient.

```
GET https://fhir.other.example/r4/metadata
```

2. Find the patient by BSN. Only POST-based search is allowed. Create the DPoP header with `htm` `POST` and `htu` `https://fhir.other.example/r4/Patient/_search`.

```
POST https://fhir.other.example/r4/Patient/_search
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Authorization: DPOP <access token>
```

```
DPoP: <dpop>
```

```
identifier=http://fhir.nl/fhir/NamingSystem/bsn|123456789
```

The result has the patient's ID at the other party, e.g. `Patient/abc123`.

3. Query the data. For example, the patient's allergies. Create a new DPOP header with

`htm` `GET` and `htu` `https://fhir.other.example/r4/AllergyIntolerance`.

```
GET
```

```
https://fhir.other.example/r4/AllergyIntolerance?patient=abc123&_profile=http://nictiz.nl/fhir/StructureDefinition/nl-core-
```

```
AllergyIntolerance,http://nictiz.nl/fhir/StructureDefinition/zib-AllergyIntolerance
```

```
Authorization: DPOP <access token>
```

```
DPoP: <dpop>
```

- Queries select resources by FHIR profile (`_profile`). [Volume 3 of the IG](#) lists the query for each zib and FHIR version.
- Results are paged: use `_count` (maximum 100) and follow the bundle's `next` link.
- The order of requests is in [volume 2b of the IG](#).

API reference: [Auth \(v2\)](#)

Revision #2

Created 2026-10-27 14:40:07 UTC by Rein Krul

Updated 2026-10-27 15:26:37 UTC by Rein Krul