Authentication & authorization

When a request comes in at your resource endpoint, an access token should be available in the HTTP Authorization header. You can validate the token by calling:

```
POST /internal/auth/v2/accesstoken/introspect


token=ciOiJSUzI1NiIsInR5cCI6Ikp
```

Note: the content-type of this call is `application/x-www-form-urlencoded`.

And the result:

```
{
  "active":true,
  "iss": "https://example.com/oauth2/other_subject_identifier",
  "client_id": "https://example.com/oauth2/my_subject_identifier",
  "scope": "coffee",
  "organization_name":"Care Bears"
}
```

Like with the discovery service, any constraint in the presentation definition of the policy file is also added as key/value pair to the introspection result. This is the mechanism to use attestations from presented credentials for authorization purposes.

The token introspection result is the last thing the Nuts node can do for you. From this point you have to apply the authorization policy...

Revision #3
Created 23 September 2024 09:28:37 by Wout Slakhorst
Updated 23 September 2024 13:56:18 by Wout Slakhorst