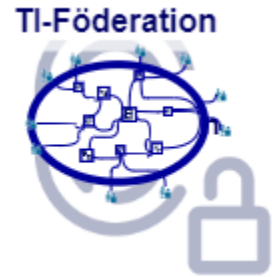


Sektoraler IDP - Referenzimplementierung und Beispiele

- Umgebungen
- Download vom GitHub
- Abholen Entity Statement



Umgebungen

Die gematik bietet eine rudimentäre Implementierung eines sektoralen IDP an. Der **gematik-eigene sektorale IDP** implementiert spezifikationskonform alle geforderten Schnittstellen. Zu Testzwecken können laufende Instanzen des **sektoralen IDP** der gematik angesprochen werden. Ebenso ist es möglich, den **gematik-eigenen sektoralen IDP** lokal zu betreiben.

In folgenden Umgebungen sind laufende Instanzen des **sektoralen IDP** der gematik erreichbar:

Umgebung	URL "issuer"	URL Entity Statement
TU Internet	https://gsi.dev.gematik.solutions	https://gsi.dev.gematik.solutions/.well-known/openid-federation

Download vom GitHub

Der sektorale IDP der gematik ist im GitHub verfügbar - <https://github.com/gematik/app-gemSekIdp>. Damit ist es möglich, den sektoralen IDP der gematik in der lokalen Umgebung zu bauen und zu betreiben.

Abholen Entity Statement

Das Entity Statement der Referenzimplementierung "gematik sektoraler IDP" kann z.B. über den Browser durch Aufruf der Schnittstelle <https://gsi.dev/gematik.solutions/well-known/openid-federation> erfolgen. Das signierte JWT sieht in etwa so aus

Header: eyJhbGciOiJIUzI1NiIsInR5cCI6ImlvbnVudGl0eS1zdGF0ZW1lbnQrand0liwia2lkIjoicHVrX2lkF9zaWcifQ

Payload:

[illegible]

Signatur: t0FQKYBue_bA2S6bOe1Cn5-F724xTA92TTPLCGDSMHTwKePd6lPkS0-6gpFtXlq2mVlrgdC5EN4i9yKulO7p4w

Nach der Decodierung bekommt man in der payload das Entity Statement des gematik-eigenen sektoralen IDP

```
{
  "iss": "https://gsi.dev.gematik.solutions",
  "sub": "https://gsi.dev.gematik.solutions",
  "iat": 1691575208,
  "exp": 1692180008,
  "jwks": {
    "keys": [
      {
        "use": "sig",
        "kid": "puk_idp_sig",
        "kty": "EC",
        "crv": "P-256",
        "x": "Abt2Uyrk6KhczexlBOwJOTs_eB0DsFbcNxaxa0Z0vd4",
        "y": "YZKBJtOUYEWTMknzFwBdl-6tVKyWnUDtxf2q0pST5X4"
      }
    ]
  },
  "authority_hints": [
    "https://app-test.federationmaster.de"
  ],
  "metadata": {
    "openid_provider": {
      "issuer": "https://gsi.dev.gematik.solutions",
      "signed_jwks_uri": "https://gsi.dev.gematik.solutions/jws.json",
      "organization_name": "gematik sektoraler IDP",
      "logo_uri": "https://gsi.dev.gematik.solutions/noLogoYet",
      "authorization_endpoint": "https://gsi.dev.gematik.solutions/auth",
      "token_endpoint": "https://gsi.dev.gematik.solutions/token",
      "pushed_authorization_request_endpoint": "https://gsi.dev.gematik.solutions/PAR_Auth",
      "client_registration_types_supported": [
        "automatic"
      ],
      "subject_types_supported": [
        "pairwise"
      ],
      "response_types_supported": [
        "code"
      ],
      "scopes_supported": [
        "urn:telematik:email",
        "urn:telematik:versicherter",
        "urn:telematik:display_name",
        "openid",
        "urn:telematik:geschlecht",
        "urn:telematik:given_name",
        "urn:telematik:geburtsdatum",
        "urn:telematik:alter"
      ],
      "response_modes_supported": [
        "query"
      ],
      "grant_types_supported": [
        "authorization_code"
      ],
      "require_pushed_authorization_requests": true,
      "token_endpoint_auth_methods_supported": [
        "self_signed_tls_client_auth"
      ],
      "request_authentication_methods_supported": {
        "ar": [
          "none"
        ],
        "par": [
          "self_signed_tls_client_auth"
        ]
      },
      "id_token_signing_alg_values_supported": [
        "ES256"
      ],
      "id_token_encryption_alg_values_supported": [
        "ECDH-ES"
      ],
      "id_token_encryption_enc_values_supported": [
        "A256GCM"
      ],
      "user_type_supported": [
        "IP"
      ]
    }
  }
}
```

```
]
},
"federation_entity": {
  "name": "gematik sektoraler IDP",
  "contacts": "support@idp4711.de",
  "homepage_uri": "https://idp4711.de"
}
}
```