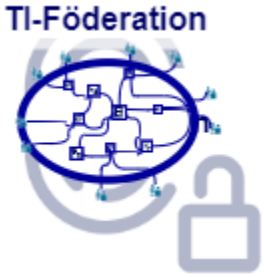
Federation Master - Umgebungen und Beispiele



Umgebungen

Umgebung	Beschreibung	URL "issuer"	URL Entity Statement
Referenzumgebung (RU)	Die Referenzumgebung ist eine Integrationsumgebung. Hier kann das Zusammenspiel der beteiligten Komponenten und Systeme überprüft werden. dazu müssen die beteiligten Komponenten und Systeme einen möglichst produktionsnahmen Zustand besitzen. Im optimalen Fall ist die Überführung in die Produktionsumgebung ausschließlich durch Konfiguration möglich.	https://app-ref.federationmaster.de	https://app-ref.federationmaster.de/.well-known/openid-federation
Testumgebung (TU)	Die Testumgebung dient der Überprüfung von Testkonzepten sowie von Schnittstellentest gegen beteiligte Komponenten. Die eigentliche Funktionalität hinter verwendeter Schnittstellen spielt eine untergeordnete Rolle. Um das Testziel zu erreichen können einzelne Komponenten durch Mock- oder Referenzimplementierungen ersetz werden.	https://app-test.federationmaster.de	https://app-test.federationmaster.de/.well-known/openid-federation
Produktionsumgebung (PU)	Die Produktionsumgebung ist für alle nutzenden Systeme und Nutzer zugänglich und muss - im Gegensatz zur Referenzumgebung - entsprechende Anforderungen an Hardware (z.B. RZ) und Sicherheit erfüllen. Für die Produktionsumgebung müssen die Produkte zugelassen werden. Je nach Produkt müssen dazu Zulassungskriterien erfüllt sein.	https://app.federationmaster.de	https://app.federationmaster.de/.well-known/openid-federation

Abholen Entity Statement

Das Entity Statement der Federation Master Referenzimplementierung kann z.B. über den Browser durch Aufruf der Schnittstelle https://app-test.federationmaster.de/.well-known/openid-federation erfolgen. Das signierte JWT sieht in etwa so aus

> *Header: eyJ0eXAiOiJlbnRpdHktc3RhdGVtZW50K2p3dCIsImtpZCI6InB1a19mZWRtYXN0ZXJfc2lnIiwiYWxnIjoiRVMyNTYifQ*
>
> *Payload:*
> *eyJpc3MiOiJodHRwczovL2FwcC10ZXN0LmZlZGVyYXRpb25tYXN0ZXIuZGUiLCJzdWIiOiJodHRwczovL2FwcC10ZXN0LmZlZGVyYXRpb25tYXN0ZXIuZGUiLCJpYXQiOjE2OTE1NTIzMDgsImV4cCI6MTY5MTYzODcwOCwiandrcyI6eyJrZXlzIjpbeyJrdHkiOiJFQyIsImNydiI6IlAtMjU2IiwieCI6IlY4T2JnVWtqZlhvblc3WEo0S2xQa2xrQjlKaUZtTi1ZbERnV055cUVtSHMiLCJ5IjoiWkNWMGEyYjYwUDZBeWw4RlBxWGhTdlJJdnVLSDZ6S1VMa3N0aEV0Wm9HcyIsImtpZCI6InB1a19mZWRtYXN0ZXJfc2lnIiwidXNlIjoic2lnIiwiYWxnIjoiRVMyNTYifV19LCJtZXRhZGF0YSI6eyJmZWRlcmF0aW9uX2VudGl0eSI6eyJmZWRlcmF0aW9uX2ZldGNoX2VuZHBvaW50IjoiaHR0cHM6Ly9hcHAtdGVzdC5mZWRlcmF0aW9ubWFzdGVyLmRlL2ZlZGVyYXRpb24vZmV0Y2giLCJmZWRlcmF0aW9uX2xpc3RfZW5kcG9pbnQiOiJodHRwczovL2FwcC10ZXN0LmZlZGVyYXRpb25tYXN0ZXIuZGUvZmVkZXJhdGlvbi9saXN0IiwiaWRwX2xpc3RfZW5kcG9pbnQiOiJodHRwczovL2FwcC10ZXN0LmZlZGVyYXRpb25tYXN0ZXIuZGUvZmVkZXJhdGlvbi9saXN0aWRwcyJ9fX0*
>
> *Signatur: G6LGRZGJDGUriltgcWft8amS33eShqUGXtj7UgEzWaSiHne-nTmrSUHLD09FHUvR9V3BP-I_QUQgx_mOM4mtUw*

Nach der Decodierung bekommt man in der payload das Entity Statement des Federation Master

```
{
"iss": "https://app-test.federationmaster.de",
  "sub": "https://app-test.federationmaster.de",
  "iat": 1691552308,
  "exp": 1691638708,
  "jwks": {
    "keys": [
     {
       "kty": "EC",
       "crv": "P-256",
       "x": "V8ObgUkjfXonW7XJ4KlPklkB9JiFmN-YlDgWNyqEmHs",
       "y": "ZCV0a2b60P6Ayl8FPqXhSvRIvuKH6zKULksthEtZoGs",
       "kid": "puk_fedmaster_sig",
       "use": "sig",
       "alg": "ES256"
     }
    ]
  },
  "metadata": {
    "federation_entity": {
      "federation_fetch_endpoint": "https://app-test.federationmaster.de/federation/fetch",
      "federation_list_endpoint": "https://app-test.federationmaster.de/federation/list",
      "idp_list_endpoint": "https://app-test.federationmaster.de/federation/listidps"
    }
  }
}
```


Öffentliche Schlüssel und Zertifikate

Das Entity Statement des Federation Master, die Liste der in der TI-Föderation registrierten sektoralen IDP und Entity Statements zu Teilnehmern der Föderation werden vom Federation Master signiert ausgegeben. Für die Prüfung der Signatur wird von den Fachdiensten und sektoralen IDPs entsprechende der öffentliche Schlüssel "puk_fedmaster_sig" benötigt. Dieser ist im Entity Statement des Federation Master unter dem Parameter "jwks" angegeben. Ein Zertifikat zum Schlüssel wird nicht mitgegeben.


```
"jwks": {
    "keys": [
     {
      "kty": "EC",
       "crv": "P-256",
       "x": "V8ObgUkjfXonW7XJ4KlPklkB9JiFmN-YlDgWNyqEmHs",
       "y": "ZCV0a2b60P6Ayl8FPqXhSvRIvuKH6zKULksthEtZoGs",
       "kid": "puk_fedmaster_sig",
       "use": "sig",
       "alg": "ES256"
     }
    ]
  },
```


Liste aller Teilnehmer der Föderation

Die Liste der in der TI-Föderation registrierten sektoralen IDP kann unter der URL, welche im Entity Statement des Federation Master unter dem Parameter "federation_fetch_endpoint" angegeben ist.

Für die Referenzimplementierung des Federation Master liefert der Browser-Aufruf https://app-test.federationmaster.de/federation/list eine Liste der registrierten Teilnehmer:


```
["https://idpfadi.dev.gematik.solutions","https://web.tu.id.digital.barmer.de/","https://gsi.
dev.gematik.solutions"]
```


Liste der registrierten sektoralen IDP

Die Liste der in der TI-Föderation registrierten sektoralen IDP kann unter der URL, welche im Entity Statement des Federation Master unter dem Parameter "idp_list_endpoint" angegeben ist, abgerufen werden. Die Liste aller Teilnehmer der Föderation kann unter der URL abgerufen werden, welche unter dem Parameter "federation_list_endpoint" angegeben ist.

Für die Referenzimplementierung des Federation Master liefert der Browser-Aufruf https://app-test.federationmaster.de/federation/listidps ein decodiertes JWT mit etwa diesem Inhalt:

Header:


```
{
  "typ": "idp-list+jwt",
  "kid": "puk_fedmaster_sig",
  "alg": "ES256"
}
```


Payload:


```
{
  "iss": "https://app-test.federationmaster.de",
  "iat": 1691590222,
  "exp": 1691676622,
  "idp_entity": [
    {
      "iss": "https://web.tu.id.digital.barmer.de/",
      "organization_name": "Verimi",
      "logo_uri": "https://web.verimi.de/images/verimi-logo-green.svg",
      "user_type_supported": "IP"
    },
    {
      "iss": "https://gsi.dev.gematik.solutions",
      "organization_name": "gematik sektoraler IDP",
      "logo_uri": "https://gsi.dev.gematik.solutions/noLogoYet",
      "user_type_supported": "IP"
    }
  ]
}
```


Fetch Entity Statement

Teilnehmer können Auskunft über andere Teilnehmer erhalten, indem sie entsprechend parametrisiert die Schnittstelle aufrufen, welche im Entity Statement des Federation Master unter dem Parameter "idp_list_endpoint" angegeben ist.

Für die Referenzimplementierung des Federation Master mit den registrierten Teilnehmern

- Referenzimplementierung eines Fachdienstes (relying party) https://idpfadi.dev.gematik.solutions
- Referenzimplementierung "gematik sektoraler IDP" (openid provider) https://gsi.dev.gematik.solutions
- Testimplementierung Barmer-IDP (openid provider) https://web.galactus.verimi.cloud/

kann der Gematik-Fachdienst https://idpfadi.dev.gematik.solutions Auskunft über den "gematik sektoraler IDP" (https://gsi.dev.gematik.solutions) vom Federation Master erlangen durch den Request:

https://app-test.federationmaster.de/federation/fetch?iss=https://app-test.federationmaster.de&sub=https://gsi.dev.gematik.solutions

die Referenzimplementierung des Federation Master liefert ein JWT mit dem Inhalt:


```
{
 "iss": "https://app-test.federationmaster.de",
  "sub": "https://gsi.dev.gematik.solutions",
  "iat": 1691591172,
  "exp": 1691677572,
  "jwks": {
    "keys": [
      {
        "kty": "EC",
        "kid": "puk_idp_sig",
        "crv": "P-256",
        "x": "Abt2Uyrk6KhczexlBOwJOTs_eB0DsFbcNxaxa0Z0vd4",
        "y": "YZKBJtOUYEWTMknzFwBdl-6tVKyWnUDtxf2q0pST5X4",
        "use": "sig",
        "alg": "ES256"
      }
    ]
  },
  "metadata": {
    "openid_provider": {
      "client_registration_types_supported": [
        "automatic"
      ]
    }
  }
}
```

Entsprechend kann der "gematik sektoraler IDP" (https://gsi.dev.gematik.solutions) Auskunft über den Teilnehmer Gematik-Fachdienst (https://idpfadi.dev.gematik.solutions) vom Federation Master erlangen durch den Request:

https://app-test.federationmaster.de/federation/fetch?iss=https://app-test.federationmaster.de&sub=https://idpfadi.dev.gematik.solutions

die Referenzimplementierung des Federation Master liefert dazu ein JWT mit dem Inhalt:


```
{
 "iss": "https://app-test.federationmaster.de",
  "sub": "https://idpfadi.dev.gematik.solutions",
  "iat": 1691591342,
  "exp": 1691677742,
  "jwks": {
    "keys": [
      {
        "kty": "EC",
        "kid": "puk_fd_sig",
        "crv": "P-256",
        "x": "9bJs27YAflMUWK5nxuiF6XAG0JazuvwRi1EpFK0XKik",
        "y": "P8lzNVROgTuwbDqsd8rT1AI3zez94HBsTDpOvajP0rY",
        "use": "sig",
        "alg": "ES256"
      }
    ]
  },
  "metadata": {
    "openid_relying_party": {
      "client_registration_types": [
        "automatic"
      ]
    }
  }
}
```