Instructions

Date
2025-05-06
Page
1 (29)
Identifier
Telia Tunnistus
Version
2.29 Approved

Approved on
May 6, 2025

Relation
Digital Identity

Approved by
Jarmo Koskimaa

Telia Tunnistus - Integration guide to identification broker service

Description
Integration guide to identification broker service

Company information
Telia Finland Oyj
Pasilan Asema-aukio 1, 00520 HELSINKI, FI
Registered office: Helsinki
Business ID 1475607-9, VAT No. FI14756079

Table of contents

1 About this document

This guide provides instructions for integrating with the Telia Identification Broker Service and enabling strong electronic identification for end users. The service supports OpenID Connect (OIDC) and Security Assertion Markup Language (SAML) protocols, offering secure authentication in compliance with Finnish regulations.

This document is intended for technical architects and developers that are looking for connecting their service to identification broker service.

1.1 Technical Contact

The customer is responsible for providing Telia Tunnistus with the contact information of a technical person for the integration.

1.2 Traficom requirements

Traficom (Finnish Transport and Communications Agency) is a Finnish government agency that is involved in promoting cybersecurity and the digitalization of services, ensuring the security of critical infrastructure and digital networks.

Interfaces between the Identification Broker Service and the customer service must comply with Traficom regulation M72B on strong electronic identification and trust services. The regulation applies to the provision and conformity assessment of devices for strong electronic identification and identification broker services that have been notified to Traficom. The SAML metadata of Telia Tunnistus is compliant with this regulation.

For more details, please see: https://www.finlex.fi/data/normit/48237/03_Regulation.pdf.

Additionally, Telia Tunnistus exclusively supports an authorization profile that complies with Traficom recommendations for attribute mapping in SAML2 assertions (212/2023 S) and OIDC ID token operations (213/2023 S).

The relying party must provide the ***ftn_spname*** to Telia. This is a short and unambiguous description of the service for the end user, which will be displayed to the end user before authentication.

1.3 Service URIs

In the production environment (which is the assumed environment in all examples of this document), the host component of endpoints and other URIs is:

tunnistus.telia.fi

In the preproduction environment, the host component is:

tunnistus-pp.telia.fi

When performing integration tests in preproduction, simply add the postfix “-pp” to the hostname in the examples provided in this document.

Information about production service disruptions is available at the following link:

https://tunnistus.telia.fi/uas/resource/maintenance.txt

Sample data:

> Aktia, Handelsbanken, Oma Säästöpankki, POP Pankit ja Säästöpankki suorittavat huoltotöitä 27.10.2024 03:00 - 10:00 välisenä aikana. Huoltotöiden aikana niiden sähköinen tunnistautuminen ei ole käytettävissä.|Aktia, Handelsbanken, Oma Säästöpankki, POP Pankit och Säästöpankki utför underhållsarbete från 27.10.2024 03:00 till 27.10.2024 10:00. Under underhållsarbetet kommer identitetstjänster för dessa bank-kunder inte vara tillgängliga.|Aktia, Handelsbanken, Oma Säästöpankki, POP Pankit and Säästöpankki performs maintenance work from 27.10.2024 03:00 - 27.10.2024 10:00. During the maintenance work identity services for those bank customers will not be available.

Language versions fi, sv, en are separated by | -character (“pipe”).

1.4 Test users

In preproduction testing, the following test users are available:

1. Mobiilivarmenne Emulator 2. Mobiilivarmenne (test)	Mobiilivarmenne Emulator: prefilled (acr value: mpki.telia.emulator.1) Mobiilivarmenne (test) needs custom provisioning to a Telia SIM card or a Mobiilivarmenne test mobile app from either Elisa or DNA
Nordea	DEMOUSER1, DEMOUSER2, DEMOUSER3 and DEMOUSER4.
Danske	88888888 / 4545
Handelsbanken	11111111 / 123456
Aktia	Prefilled
Ålandsbanken	12345678 / 123456 / 1234 (choose code card option)
S-Pankki	12345678 / 123456 / 1234 (choose code card option)
OP	Prefilled
Säästöpankki	11111111 / 123456
POP	11111111 / 123456
OmaSP	11111111 / 123456

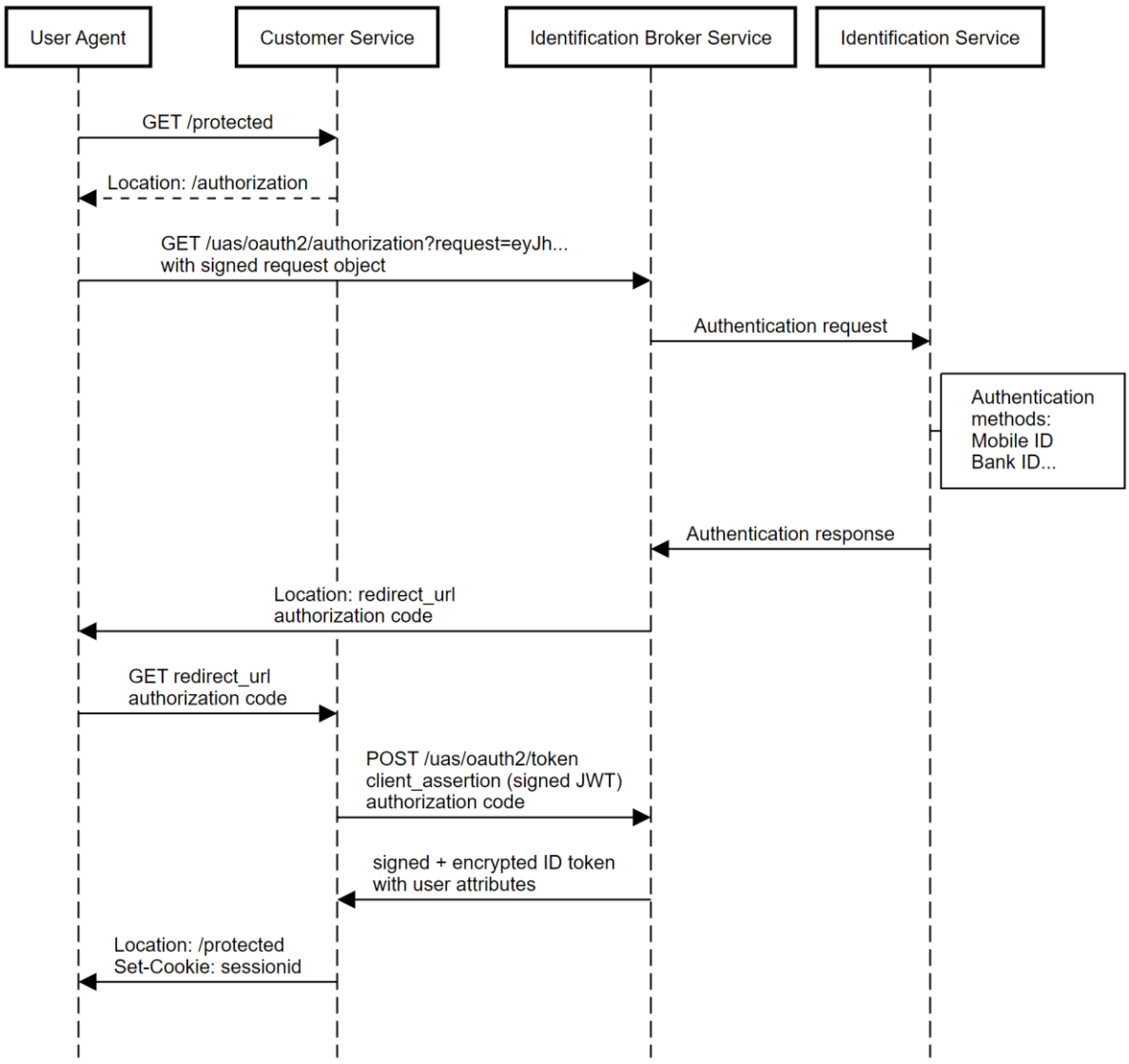
2 OpenID Connect

Here are the instructions for setting up OpenID Connect integration with the Telia Identification Broker Service (Telia Tunnistus).

OpenID Connect integration allows the customer service to request that the end user perform strong authentication using any of the supported authentication providers by the identification broker service. For example, customer service may request the end user to authenticate using Mobile ID or Bank ID.

In a web single sign-on use case, a single OAuth client is registered with the identification broker service. This client is a web application running on a web server. The client seeks to obtain an ID token with the user attributes included. The ID token contains claims and attributes describing the authenticated user.

Only the authorization code grant and web single sign-on use cases are supported..



More details about OpenID Connect is available in:

- The OAuth 2.0 Authorization Framework: https://tools.ietf.org/html/rfc6749 and https://tools.ietf.org/html/rfc6750
- OpenID Connect Core: http://openid.net/specs/openid-connect-core-1_0.html
- Client Assertion: https://datatracker.ietf.org/doc/html/rfc7523
- Signed Request Object: https://datatracker.ietf.org/doc/html/rfc9101
- PKCE: https://datatracker.ietf.org/doc/html/rfc7636

2.1 OIDC client registration

A technical contact person, authorized to establish an encrypted connection with the Telia Identification Service and handle key exchanges, can be found in Appendix 4 of the Telia Identification Service Agreement.

Key exchanges must only be conducted with the designated individual, whose contact information is listed in the agreement.

Telia Tunnistus will need following data from the client:

2.1.1 Public keys

Client public keys are required for ID token encryption, signed request object verification, and client assertion signature verification on the Telia Tunnistus side.

The public keys must be provided to Telia Tunnistus via secure email, JWKS URI, or Entity Statement (OpenID Federation).

The keys should use the RSA algorithm, with a minimum key length of 2048 bits. The client must provide separate public keys for signing (“use”: “sig”) and encryption (“use”: “enc”). *See Section 2.3, Client Public Keys.*

2.1.2 Entity Statement (optional)

An alternative method for the client to provide its OIDC public keys (signed JWKS) is by submitting its OpenID Federation Entity Statement to Telia Tunnistus, either via secure email or by publishing the OpenID Federation endpoint to Telia Tunnistus.

2.1.3 Redirect URI(s)

Clients are required to provide at least one HTTPS URL (redirect URI) of the client service. Multiple redirect URIs can be specified, but wildcard entries (e.g., https://example.com/*) are not supported. Ensure that all URIs are properly registered.

2.1.4 Service display name

Client must provide a ***display name*** (ftn_spname). This is mandatory for clients that use Finnish strong authentication (FTN) methods. The relying party must provide a short (max. 40 characters) and unambiguous display name of the service to help end user to identify the service. This name will be shown to the end user during the authentication process.

2.2 Endpoint locations

Telia Identification Broker Service has the following OpenID Connect endpoints:

Environment	Address
Production	*https://tunnistus.telia.fi*
Pre-production	*https://tunnistus-pp.telia.fi*

Endpoint	URL
The well-known OpenID Connect Federation Entity Statement	*/.well-known/openid-federation*
The well-known OpenID Connect provider metadata endpoint	*/uas/.well-known/openid-configuration*
The well-known OAuth 2.0 provider metadata endpoint.	*/uas/.well-known/oauth-authorization-server*
Public keys	*/uas/oauth2/metadata.jwks*
Public keys in signed jwks format	*/openid_provider/signed_jwks.jwt*
Authorization Endpoint	*/uas/oauth2/authorization*
Token Endpoint	*/uas/oauth2/token*

2.2.1 SHA256 hash/fingerprint values for Entity Statements

Endpoint URL	SHA256 value
https://tunnistus.telia.fi/.well-known/openid-federation	1e8ba3d6cd534a8199ef0596ce94fece75c58d40d990c7e8ea792b99affc762c
https://tunnistus-pp.telia.fi/.well-known/openid-federation	2bb459b631d4c157f91ef7858d7f5baec6961d1d59df1b61eff7ae6905061cda

Examples for out-of-band validation of Entity Statement:

Linux Bash:

```
# First download entity statement with curl:
curl -s https://tunnistus.telia.fi/.well-known/openid-federation -o openid-federation

# Then check SHA256 fingerprint with sha1sum:
sha256sum openid-federation

# Output from command is:
1e8ba3d6cd534a8199ef0596ce94fece75c58d40d990c7e8ea792b99affc762c openid-federation
```

PowerShell:

```
# First download entity statement with Invoke-WebRequest:
Invoke-WebRequest https://tunnistus.telia.fi/.well-known/openid-federation -OutFile openid-
federation

# Then check SHA256 fingerprint with Get-FileHash:
Get-FileHash openid-federation -Algorithm SHA256
```

```
# Output from command is:
Algorithm   Hash                                                             Path
---------   ----                                                             ----
SHA256      1E8BA3D6CD534A8199EF0596CE94FECE75C58D40D990C7E8EA792B99AFFC762C  openid-federation
```

2.3 Client Public Keys

Client public keys are needed for **ID token encryption** and **signed request object and client assertion signature verification** on Telia Tunnistus side.

The client should provide separate public keys for signing (“use”:”sig”) and encryption (“use”:”enc”).

2.3.1 Public keys sample


```
  {
      "keys": [
          {
              "e": "AQAB",
              "kid": "34567947-2167-4a9c-8368-b199fe63b6e2",
              "kty": "RSA",
              "n":
  "yas1HSwbF85dr4YpMOlcupdZY4SEBPrCZMp5w6F9IxWewmhQSsa1fGa2t3_CKl0LgIM1nbJd1fr5CQKN_Hpb0u7H5N3Not4akhNqcZHGNI7xrwOn
  OOIifwgQb2SF3J7xtKJJ0s8igQ5gxNm5rJyaeeJFxoR3tZC9lMbBpHdOiH7HXz3OOZIDbFm5da-
  i2u91T22UJgHBIZmXzl_7L3ZpIenSECRD9M3fuj9aVCNf3zKo67UuqaPdueRj_ywGqk94Iwr-FnmZ9NKpZe067VK4s2h-
  CufkGCAhKu9WVgSIHzSzIzCbLSfTXgMCpJyC4dw7TBzlvHOI3BgMjqrUqb3kkw",
              "use": "sig"
          },
          {
              "e": "AQAB",
              "kid": "ae29278f-87be-4914-bcfc-bdb659e8fe1d",
              "kty": "RSA",
              "n": "wDYW8Y_uZI9F9Qy0WrwYE6xkxEF8k4PTMUgl-ul3J7Lw-v9VuZtH2aSoX3LgTH_qpCGRIUZy7OPDYYXGV1phrVHs7-
  NpevO4aXdTZOwUvjViFbTXO3RkTdh4f0d_YpA6RC2owI41BhE_FmShmPKNGskpyTNAp1E_eH1e_w4FM2g_sbwlDJQ1ckJSyXkDoGrW7Dbx34zlrQg
  UgHdKtepSCX_b3WWLKD3KW7W3lmoeSpI9iLmPLJMiYHlBcd70dCBBQW24n2bSk1BLwiNVETWPfsNnFWA2t19Jl0u3vCHNCCdKi0WORtI-
  JiaXQSmPW9ZD2kiZUwYwRi8Cg6Z9a85ngQ",
              "use": "enc"
          }
      ]
}
```

2.4 Authentication Request

An authentication request is an OpenID Connect authentication request that requests the end user be authenticated.

Telia Tunnistus requires authentication request to be sent as ***signed request object*** (also known as Secured Authorization Request).

2.4.1 Required authentication request query parameters

Parameter	Note
request	This is the signed request object. It represents the request as a JWT whose claims are the request parameters. This JWT is called a Request Object.

2.4.2 Required JWT claims in request object

Parameter	Type	Note
iss	string	OAuth Client Identifier of the web application. This value is generated by Telia Identification Broker Service when the OAuth Client is registered and activated. It has the same value as client_id.
aud	string or array of strings	Audience; use the value **https://tunnistus.telia.fi/uas** in production or **https://tunnistus-pp.telia.fi/uas** in pre-production environment
response_type	string	For authorization code grant the value must be set to "*code*"
scope	string	For web single sign-on use case the value is set to "*openid*"
client_id	string	OAuth Client Identifier of the web application. This value is generated by Telia Identification Broker Service when the OAuth Client is registered and activated.
redirect_uri	string	The redirect uri value must have been registered with identification broker service. The identification broker service redirects the web browser to this address after authenticating the end user. Wildcards are not supported.
acr_values(*)	string	(*)This is mandatory when using an authorization profile compliant with Traficom recommendation 213/2023 S. In that case the value must be: "*http://ftn.ficora.fi/2017/loa2*".

2.4.3 Optional JWT claims parameters

Parameter	Type	Note
exp	int	Expiration time after which the request object is no longer valid. Numeric value representing the number of seconds from January 1, 1970, at 00:00:00 UTC until the specified UTC date/time (UNIX epoch time). Suggestion: 10 minutes in future.
jti	string	JWT ID; the jti claim is used to prevent the request object from being replayed
state	string	An opaque value used by the client to maintain state between the request and callback
nonce	string	An opaque value used to associate a client session with an ID Token, and to mitigate replay attacks
acr_values	string	Choose authentication methods that may satisfy the request: Finnish Trust Network (FTN): mpki.telia.1 Mobiilivarmenne

Parameter	Type	Note

mpki.telia.emulator.1	Telia Mobiilivarmenne Emulator (Pre-prod)
oidc.aktia.1	Aktia
oidc.alandsbanken.1	Ålandsbanken
oidc.danskebank.1	Danske Bank
oidc.handelsbanken.1	Handelsbanken
oidc.nordea.1	Nordea
oidc.omasp.1	Oma Säästöpankki
saml.op.1	Osuuspankki
oidc.pop.1	Pop Pankki
oidc.sp.1	Säästöpankki
oidc.spankki.1	S-Pankki
oidc.hightrust.id.1	Hightrust.id

If only one authentication method is included then identification broker service initiates that authentication method automatically, if available.

If no authentication method is indicated, then the following acr_value should be used:

http://ftn.ficora.fi/2017/loa2	Production
http://ftn.ficora.fi/2017/loatest2	Pre-Production

Other methods:

Following methods need **additional order**. Contact here.

Henkilökortti in Finland:

- pki.hst.1

Value <rpname> is application/client -specific and created by Telia specifically for the customer.

Bank ID Sweden:

- oidc.<rpname>.bankidse.1

Bank ID Norway:

- oidc.<rpname>.bankidno.1
- oidc.<rpname>.bankidno.2

MitID in Denmark:

- oidc.<rpname>.mitiddk.1

Smart-ID or Mobile-ID in Estonia, Latvia and Lithuania:

- oidc.sk.1

Parameter	Type	Note
ui_locales	string	Choose the locale used in the login form: “*fi*”, “*sv*”, or “*en*”.
max_age	string or int	Specifies the allowable elapsed time in seconds since the last time the user was authenticated. If the elapsed time is greater than this value, the user is re-authenticated; value “0” indicates “force-authn”.
prompt	string	Possible values: *none*, *login*. Value none means that the user is not shown a login page at all, which means that user won’t be attempted to authenticate unless they already have an existing authentication. Value *login* means that user is always shown a login page, despite having an existing authentication or not.

2.4.4 Signed authentication request sample

```
https://tunnistus-
pp.telia.fi/uas/oauth2/authorization?request=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ
9.eyJhdWQiOiJodHRwczovL3R1bm5pc3R1cy1wcC50ZWxpYS5maS91YXMiLCJjbGllbnRfaWQiOiIwMD
QzYjQyNi0yZTZkLTQ2NmQtYjgyZi0zM2JiN2QzY2I2ZWEiLCJpc3MiOiIwMDQzYjQyNi0yZTZkLTQ2Nm
QtYjgyZi0zM2JiN2QzY2I2ZWEiLCJyZWRpcmVjdF91cmkiOiJodHRwczovL2V4YW1wbGUuY29tL3JlZG
lyZWN0IiwicmVzcG9uc2VfdHlwZSI6ImNvZGUiLCJzY29wZSI6Im9wZW5pZCJ9.IlnDUI0LsaKgwewyG
m_YieGbXAl-Xd9nKKC7Ee868medKk_CuBLEmjWQGIvSePUT7ML-bLd2cYc_loDoCvpjfAvxMI_ZDLe9-
GE-v1njUHYgtW54YyC4tKpNii9VXLlavDNLlzq55mA1r0wpn_VOj68qLeJjFHua-
CVZsbfYIYBdCqjV_vg6ikBeHVNdlO1jV6M2uWNAPSlGIaYc5IjRNzCpCs1Pwg0J50zRMiOkmuRSk0iyt
qjoIJYU_j6IWhJvPWyLWcmXdqnmzumYJq_vYoKFnLeD-
ejrRR749usWU42kmk91eqUy6sNdP7k9pXG9J9KNXybgURUzIeG_RmZGBQ
```

The **request object** is signed JSON Web Token (JWT) that consists of:

Request object JWT header:

```
{
  "alg": "RS256",
  "typ": "JWT"
}
```

Request object JWT payload:

```
{
  "aud": "https://tunnistus-pp.telia.fi/uas",
  "client_id": "0043b426-2e6d-466d-b82f-33bb7d3cb6ea",
  "iss": "0043b426-2e6d-466d-b82f-33bb7d3cb6ea",
  "redirect_uri": "https://example.com/redirect",
  "response_type": "code",
  "scope": "openid"
}
```

2.4.5 Authentication request with specific authentication method sample

The following sample authentication request contains optional parameter *acr_values* to indicate a specific authentication method to be used. Identification broker service initiates authentication with the specific authentication method.

NOTE: Clients that call authentication methods by using acr_values should regularly check if there are changes regarding the available methods.

```
https://tunnistus-
pp.telia.fi/uas/oauth2/authorization?request=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ
9.eyJhY3JfdmFsdWVzIjoib2lkYy5ha3RpYS4xIiwiYXVkIjoiaHR0cHM6Ly90dW5uaXN0dXMtcHAudG
VsaWEuZmkvdWFzIiwiY2xpZW50X2lkIjoiMDA0M2I0MjYtMmU2ZC00NjZkLWI4MmYtMzNiYjdkM2NiNm
VhIiwiaXNzIjoiMDA0M2I0MjYtMmU2ZC00NjZkLWI4MmYtMzNiYjdkM2NiNmVhIiwicmVkaXJlY3RfdX
JpIjoiaHR0cHM6Ly9leGFtcGxlLmNvbS9yZWRpcmVjdCIsInJlc3BvbnNlX3R5cGUiOiJjb2RlIiwic2
NvcGUiOiJvcGVuaWQiLCJ1aV9sb2NhbGVzIjoiZmkifQ.UQMY-
Bq8gAdOGl1wtBOphLHeswK6oOqqMJF5VDAps2c37GOEqdMMmh3ubnQt9Uems3V2rA7Y5a2RAmaCci1Pl
qarHJ5acjU1LM5-
VkE8dTcvqtzS6Ei64kid5PITvt99pGULRbFRKZAVEq5sJvisG9iUwdqZvsAVhpnC0trrqssOID7ofB8A
```

3GLoiTl0uWX1PtjP-ETkeqnKUcohh2raUC_R41vl2_gBsMulDYNalLrijDKJ08Wdn7cMZeaxXnwwGnPdggr06rndpFhZv6QpBz8xu2FjNHa9p-YtpsyxoFjaYCzBvOlRm7QhrEJJgkPJCoDhnWx3Q_dbJbJmNWaLZQ

The data in the **JWT object**:

Authorization request JWT header:


```
{
        "alg": "RS256",
        "typ": "JWT"
}
```


Authorization request JWT payload:


```
{
        "acr_values": "oidc.aktia.1",
        "aud": "https://tunnistus-pp.telia.fi/uas",
        "client_id": "0043b426-2e6d-466d-b82f-33bb7d3cb6ea",
        "iss": "0043b426-2e6d-466d-b82f-33bb7d3cb6ea",
        "redirect_uri": "https://example.com/redirect",
        "response_type": "code",
        "scope": "openid",
        "ui_locales": "fi"
}
```


2.5 Authorization Response

Authentication response sample

https://example.com/redirect?code=**eyJjdHkiOiJKV1QiLCJhbGciOiJkaXIiLCJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiemlwIjoiREVGIiwiaXNzIjoiMDA0M2I0MjYtMmU2ZC00NjZkLWI4MmYtMzNiYjdkM2NiNmVhIn0..Zq_SWe5dOcB_dpR8kf_uzA.JvGw9VeZjtk4nhsvNI29PvkCwAyq9hg8TXZEACJzDlg_UaOYCRMr9pZZDYOHzNEgwRRWajNGr4gCFi6IKJaV6HV-22A1bnyhJzkJhxfpJzYQFnjCZcsXWscO6OGY9lj9W23iviB4jlx9yTe8Ee8nkL3ldcVWsy4x29SHkTzMPFJXr76TMQwLCe0Gj8gFD2FMYaz7MLrZIbArbnM9hMfYc8d7eO6sfEVEac845GUijHM06o7pTb1J8qSw1gw21UiavN8GMA9SCTYLCGAyD2p5cfzUpBi7vE5yI1mmLEf_SB0pXwb9AIMMm3UzZKj69MMshG7WDhwAwrNlCrumr9sgjg.sCF_Jn1LB3cLRi8eRWGLwA**

2.5.1 Parameters

Parameter	Note
code	Authorization Code value generated by identification broker service

2.5.2 Optional parameters

Parameter	Note
state	Value from authorization request
error	Value is “access_denied” and parameter “code” is omitted if user cancels authentication

NOTE: There is no need to perform cryptographic operations on the **authorization code**; it should be transmitted as is.

2.6 Token Request

To obtain the ID token, the customer service sends a token request to the token Endpoint. Client authentication is performed using the “private_key_jwt” authentication scheme. The token request contains the parameter “client_assertion” which is a JWT signed with the RS256 algorithm and using the client’s private key.

2.6.1 Required parameters

Parameter	Note
grant_type	For token request with authorization code the value must be set to “authorization_code”. Allowed by default.
redirect_uri	The value must be the same that was used for authorization request.
code	Authorization Code value received in Authorization Response.
client_id	OAuth Client Identifier.
client_assertion_type	urn:ietf:params:oauth:client-assertion-type:jwt-bearer
client_assertion	Contains a signed JWT.

2.6.2 Required JWT claims in client_assertion

Name	Type	Description
iss	string	Issuer; use **client_id** of your client
sub	string	Subject; use **client_id** of your client
aud	string	Audience; use the token endpoint value **https://tunnistus.telia.fi/uas/oauth2/token** in production or **https://tunnistus-pp.telia.fi/uas/oauth2/token** in pre-production environment
exp	int	Expiration time after which the request object is no longer valid. Numeric value representing the number of seconds from January 1, 1970, at 00:00:00 UTC until the specified UTC date/time (UNIX epoch time). Must not be more than 60 minutes into future, otherwise the request will fail.
jti	string	JWT ID; the jti claim is used to enforce one-time use of JWTs

Client assertion JWT header:

```
{
        "alg": "RS256",
        "typ": "JWT"
}
```

Client assertion JWT payload:

```
{
        "aud": "https://tunnistus-pp.telia.fi/uas/oauth2/token",
        "exp": 1746184458,
        "iss": "0043b426-2e6d-466d-b82f-33bb7d3cb6ea",
        "jti": "72b11a11-9584-4311-b5fa-423f33017c62",
        "sub": "0043b426-2e6d-466d-b82f-33bb7d3cb6ea"
}
```

Token request sample

```
POST https://tunnistus-pp.telia.fi/uas/oauth2/token HTTP/1.1
Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code&code=eyJjdHkiOiJKV1QiLCJhbGciOiJkaXIiLCJlbmMiOiJBM
TI4Q0JDLUhTMjU2IiwiemlwIjoiREVGIiwiaXNzIjoiMDA0M2I0MjYtMmU2ZC00NjZkLWI4MmYtMzNiY
jdkM2NiNmVhIn0..Zq_SWe5dOcB_dpR8kf_uzA.JvGw9VeZjtk4nhsvNI29PvkCwAyq9hg8TXZEACJzD
lg_UaOYCRMr9pZZDYOHzNEgwRRWajNGr4gCFi6IKJaV6HV-
22A1bnyhJzkJhxfpJzYQFnjCZcsXWscO6OGY9lj9W23iviB4jlx9yTe8Ee8nkL3ldcVWsy4x29SHkTzM
PFJXr76TMQwLCe0Gj8gFD2FMYaz7MLrZIbArbnM9hMfYc8d7eO6sfEVEac845GUijHM06o7pTb1J8qSw
1gw21UiavN8GMA9SCTYLCGAyD2p5cfzUpBi7vE5yI1mmLEf_SB0pXwb9AIMMm3UzZKj69MMshG7WDhwA
wrNlCrumr9sgjg.sCF_Jn1LB3cLRi8eRWGLwA&redirect_uri=https%3A%2F%2Fexample.com%2Fr
edirect&client_id=0043b426-2e6d-466d-b82f-
33bb7d3cb6ea&client_assertion=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJod
HRwczovL3R1bm5pc3R1cy1wcC50ZWxpYS5maS91YXMvb2F1dGgyL3Rva2VuIiwiZXhwIjoxNzQ2MTg0N
DU4LCJpc3MiOiIwMDQzYjQyNi0yZTZkLTQ2NmQtYjgyZi0zM2JiN2QzY2I2ZWEiLCJqdGkiOiI3MmIxM
WExMS05NTg0LTQzMTEtYjVmYS00MjNmMzMwMTdjNjIiLCJzdWIiOiIwMDQzYjQyNi0yZTZkLTQ2NmQtY
jgyZi0zM2JiN2QzY2I2ZWEifQ.M0ubXkK0IbXzY9On3GOabX-FzUZsL8Pesz-
0TsdtShWwAky9dG_CKYMaarRwnk9zUPIrxyYA5ga5j-q8wYSbvIJDJ9Han-
NOhZDy_UB9gPDrB4dAYqgHGmqF8KRb61p25qqSf3U016PbQb71lUe_Q9ullT-
65CJ3FLL8qjUtfDQRM_U--oOdPfpz1cc2Z-
```

```
bvA1mbfRih_sSkdDImkR25FN4xSZtPXUiuIUAWxaxz63TYHDfREqpJFMDxN2MzWFwn4nHQHtBrM7a8J-
V7ncex848VmQYnEgdNNNcj7zzFNuqkgU34mw6qpDBZS9u-H5Q3WC8X-
A802FP7AbcHpHnQsg&client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-
assertion-type%3Ajwt-bearer
```

2.6.3 Token response parameters

Parameter	Note
scope	scope = openid.
expires_in	The lifetime in seconds of the access token
token_type	token_type = Bearer
access_token	Access token issued by the identification broker server. Access tokens are not used in Telia Tunnistus authentication context.
id_token	id_token is always returned and contains the identity claims. Id_token is a JWT encrypted with the client's public key and signed with Telia's private key. The client must decrypt the ID token with its private key, and the client must verify the signed JWT with Telia's public key.

Sample token response

```
HTTP/1.1 200
Content-Type: application/json;charset=UTF-8

{
        "access_token":
"eyJjdHkiOiJKV1QiLCJhbGciOiJkaXIiLCJlbmMiOiJBMTI4Q0JDLUhTMjU2IiwiemlwIjoiREVGIiwiaXNzIjoiMDA0M2I0MjY
tMmU2ZC00NjZkLWI4MmYtMzNiYjdkM2NiNmVhIn0..n3McPWV_nSZjfuaZpEgVRw.LFQGZUHHb1Nz2YW9vN-7agW-
2nbuPZYc5UvIThQVK3YfCAZrOmoDZPvMFxyVVL7w0H39KpIJzm-
0sAG1eaxFcWvz02TfajY8MGRCpSSuDOIsomJOu5m2GIhI3y3p7pM5J4RDsvGAwmdXQM1gJTyqH5rOW1fPTV_2QLHB_pOP72_UEoD
bFtQoad6AmlEFZeuXxlvV76bydLkHRO-dIYzKzd1kiqbcU0N6TvP9z-kjFW-
pAOvasrr_eI_0drThK1JSHEaHZFaujwiqNHpTuXDWRI4k3MCo25pfyEurZVGZm5KKem0lwXQ2d0E_nGl-mxUPdLrjWSPH1VJU--
RwjCR8R7zJhmia-URHZQQIXhZ1M8VNrudLxL___Ab8MgQWr-09.rZCr-Yo4wRw8VmwwqJ0uVg",
        "scope": "openid",
        "id_token":
"eyJjdHkiOiJKV1QiLCJhbGciOiJSU0EtT0FFUCIsImtpZCI6ImY0MWMzN2Q0LTIyMDEtNGNiNC05YTE0LWExNmFkZTc5YTk1MCI
sImVuYyI6IkExMjhDQkMtSFMyNTYifQ.IMfl5rs 43zpc4rvwHNDKzon76u19M2C4Ylth1n7C8qjEXuqYaBo9R MXCA8FvFRiqbv
XGhY15Z9qe0_5aRbHqaJygXkh7qHpHQ8Ein8nuNj1caT9x0PR9HGoA1xsYErNGuywx_MXpXzkVTTown-
gCkquZVvimAeo5MeEPR2pYRWDhjlOrAOo6UX3OYinZYnPdptWTMvWv8gT8ElqQ7qnUcurwwnEWBDaKeSfsw9GVfS2V_q6Kg-
CMcIbHnTpSTSLQe7Ei0moExanqsNsGnuGKZJm1WO07ULJaO2mpZIYqJa94lb2CKu3KQMuZaXNWhLYX920eHRkvE9etPy2LzbTQ.Y
s9GVLdJgg1QR8XDFdgTLw.gM287LIIobIaYiNqro40oPd-mBfx1AXCTjCn61Rvp6YPKZg0pwk38kCQS3-
Cw9VJI1skz0tZlkMO483qiG57XxyDQ1aCvYwEquh36GGagci3nKV2sNeRqHfvBOcBfaOttTYjB4hiZ dEyVPHfXhCU7 -
5Otg5LnDM1Y_oMiVN4sH_gNtpRj6JeApuaUIDkFO-
FYNxDjlIf_ow1Xwo2D2Nfu3IwLt2wbV32Wqdm7mDdGZRfSaJSaLye5xNCJ3pQfREKIqfL4rFVLI26vBtNcz2LL7dIuoWgpcHKinU
sJebJP9_pfVqPFpwJzgQ2z41JANf_1IRpLRmylTm1OGmW4o8iRC_Gd2YT8PloX4h2i33bn7SrP63dta3txypMVzwGdcsE8PIILos
IQMLJbHi6LmkCW0-uwBZ2ZmBViW7lpXICtHWPRR_RQxIol2vn9-JLA5sFxCUp9Tg8S0rTHj4Tz1mOjbk2k-
pNmpCiBx8z4noJxRJ4fyBsNUReiZ6ueqbrUOWjiDmwVl1ai6kEEg69433IH7sz9Wt3pJoAO3znAZwmx1z7n0m2fmQ3MjLvU9lrCn
aV8-
Hu91Rc4CkEtNm75MfzpuG2lXayKWnV99_HmutRLpN1fFu6VMyS_XESdtHgXCyEvcYIi8wbyxLg6xz0gEZbUpNRFODuMLptdsjnBk
_zrf9DJxjSwa6TRI2rCUOgBKH2JHaL3sUDzH1fkHjNNjTfKr4ZU6tjKjU7dkzSWVWut4JGuZw6rVUCvSnJwVe9AX1sRjgcnN0Qh2
G_rHLw85qvaGnAjLpSAO_C9-Zj7bTmhmrnnCs5mXfVsFSyqMfl_EcgRqDB3hH5dzSnTHg0QJarv-
o5ZKZ9kkIA3AsuvfOItaC9bLdtMZVQ72sYkr6hNXIpHLjdE6HaK7ScOqZ-
c4IuO1h0nh88fjdloHGbOHeCwubqfre3A3fSamaQxYTyG9JULrEFM5mUrXClZ00M9aewDYo_gOJYL1rQbVe5mCoGQ6cw0Pfq-
oxl9M0JHoo1ygdR4djP-2L5xCE1yH-NIjzjKyxiYv2gi32BYbEbGfzxky_5TvlqbBzIKo9HfO6WEJ-
UEfeVJ1XWCZhWxo4h4dTdEV00WlTDtWwtuk07Gu8xf7rGFHragdkdtFN45furAQm_kqWr9cYEg2NlTFoMTz_5l7iLAP6U30HIg54
TXkZLV9WyyBZTlX1Lnu1c6bt9BY79wetoCTR_XB7WZW6C4hN7UUkooXeP0sLceOEExPhbOlxzIxoWLiCFou2WzWyjtHflElU9Ta4
4azqGpSKxKtnTNeLPHdWtOcB6Xu02vYzMS5hUYRoU128dddc-
AeNF0rFEtVIXUvkMGh5X9Hn_uPAED5X6mWz_hQy3hus_2y0uGloDtHp80YGSXa4ZJ2ORjAeErZFLvMIko1EmQHlvBh_14oFnl-
OtgAuM0GAZyukAfyp6PtwDF084fvGGrc-XAdHPH8Bbdp5pj3EFwlQ4x3fhtCafSTji-RdrsS-FIUl85gkW5ejWM7ljpJvJjKoWT-
```

```
T_pGuMHHG-dq-
yvNpSnt0H_TUHxf0Uz2tQGBhlBhPcqWratnsrsr9dC9dGAH0LX_KTQ0zNSBiAq2TfRF_6lr5sU2DLeHD4Wp1yx5LlY7xrGgvpZOB
jHVCEjXEnNr__cnH1-fZ4BBLV6eZzYUF-Vl1F12JvJiX5nwJsUKK-CDLENLIo8khqWZ6qgJVUg8fYDFffO5CrUfZB-
E9K_G43D2bgJS4Slpc5fEBMpHmVawfEPUKy8QS5_dk_hxFQoqnH5K.GX1BZRHmcQBYjve70PkKGQ",
        "token_type": "Bearer",
        "expires_in": 600
}
```


2.6.4 ID token payload claims (Finnish users via FTN methods)


```
{
        "sub": "2BY5CDNFBEOSUFSKNGFSY4Y3DZISGL4I",
        "iss": "https://tunnistus-pp.telia.fi/uas",
        "aud": [
            "0043b426-2e6d-466d-b82f-33bb7d3cb6ea"
        ],
        "exp": 1746184457,
        "iat": 1746183858,
        "auth time": 1746183857,
        "acr": "http://ftn.ficora.fi/2017/loatest2",
        "amr": [
            "https://tunnistus-pp.telia.fi/uas/saml2/names/ac/oidc.aktia.1"
        ],
        "azp": "0043b426-2e6d-466d-b82f-33bb7d3cb6ea",
        "session_index": "_cb08aaa8c860fed8c798aac35885f4004fe15bb5",
        "urn:oid:1.3.6.1.5.5.7.9.1": "1970-01-01",
        "urn:oid:1.2.246.21": "010170-999R",
        "urn:oid:2.5.4.4": "Äyrämö",
        "urn:oid:1.2.246.575.1.14": "Tero Testi",
        "urn:oid:2.16.840.1.113730.3.1.241": "Tero Testi Äyrämö",
        "bank-tupasid": "Aktia-saastopankit-paikallisosuuspankit-tupasid"
}
```


Name	Description
iss	“https://tunnistus-pp.telia.fi/uas”
aud	Client_id of the customer service
exp	Expiration time (epoch time)
iat	Issued at time (epoch time)
auth_time	Timestamp of user authentication (epoch time)
nonce	Value from authorization request
acr	http://ftn.ficora.fi/2017/loatest2 (production: http://ftn.ficora.fi/2017/loa2)
amr	Method reference in URI format
urn:oid:1.3.6.1.5.5.7.9.1	Date of Birth ‘YYYY-MM-DD’
urn:oid:1.2.246.21	Finnish Personal Identity Code
urn:oid:2.5.4.4	Surname
urn:oid:1.2.246.575.1.14	Given name

2.6.5 ID token payload claims (Non-Finnish users)

Name	Description
iss	“https://tunnistus-pp.telia.fi/uas”
aud	Client_id of the customer service

Name	Description
exp	Expiration time (epoch time)
iat	Issued at time (epoch time)
auth_time	Timestamp of user authentication (epoch time)
nonce	Value from authorization request
amr	Method reference in URI format
urn:oid:1.3.6.1.5.5.7.9.1	Date of Birth ‘YYYY-MM-DD’ (only MitID Denmark, Norway BankID)
http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier	National person identification code
urn:oid:2.5.4.4	Surname
urn:oid:1.2.246.575.1.14	Given name

2.7 Key Management

2.7.1 Key Rotation

Telia Tunnistus may rotate its signing keys occasionally. When key rotation is planned, Telia Tunnistus will publish the next signing keys well in advance in its public keys metadata endpoints. Telia Tunnistus will inform customer’s technical contact about the changes beforehand.

The client must have capability to consume new keys when needed.

2.7.2 OpenID Connect Key Management

Telia Tunnistus supports OpenID Connect Federation Key Management, see 2.1 Endpoint locations and Traficom Recommendation 213/2023 S.

3 SAML

Here are the instructions for setting up the SAML integration in the Telia identification broker service (Telia Tunnistus). SAML integration allows customer service to request end user to perform strong authentication using any of the supported authentication providers by the identification broker service. For example customer service may request end user to perform Mobile ID authentication or Bank ID authentication.

In a web single sign-on use case a single SAML Service Provider is registered with the identification broker service. SAML SP sends a SAML authentication request and receives a SAML authentication response from identification broker service containing agreed user attribute statements.

3.1 SAML client registration

A Service Provider has to be registered to identification broker service before it can act as an identification broker service to the SP. Registration happens by importing the SP's SAML metadata.

The general format of metadata describing the Service Providers configuration and supported features is described in SAML 2.0 metadata.

The entityID must be a globally unique string that identifies the client service. It is recommended to use a URL format (e.g., https://yourservice.com/saml2).

Regardless of whether the Service Provider chooses to set the *AuthnRequestsSigned* attribute to *true* or *false*, identification broker service will never accept an unsigned authentication request.

The SP must provide one RSA public key that it will use to sign requests. For Service Providers there must be an assertion consumer service endpoint using POST binding and a single logout endpoint using either Redirect or POST binding or both.

3.2 Metadata

Telia Identification Broker Service metadata can be downloaded directly from the service, using the metadata distribution URL of the service (for example, `https://tunnistus.telia.fi/uas/saml2/metadata.xml`).

The authentication requests have to be signed (as described by WantsAuthnRequestsSigned attribute) and the metadata will always have one ORSA public key that identify broker service uses for signing the responses and assertions. The metadata will also list supported single sign-on bindings and locations. Service Provider will use the POST binding or Redirect Binding for the authentication and logout requests.

For a detailed description of the SAML 2.0 metadata, please refer to http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.

3.3 Authentication request

See following references for more details for description of the SAML WebSSO authentication and logout process using POST and Redirect bindings.

- Profiles for the OASIS Security Assertion Markup Language (SAML) http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
- Bindings for the OASIS Security Assertion Markup Language (SAML) http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

The authentication requests that the SP sends to identification broker service may have isPassive attribute set if the Service Provider wishes to check whether the user has an existing session at identification broker service. The format is as described in the SAML standards.

Sample authentication request

```
<samlp:AuthnRequest xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

Destination="https://tunnistus.telia.fi/uas/saml2/SingleSignOnService"
                    ID="_487a3cd30d7778d5665b6b13db908d35b8e594bc"
                    IssueInstant="2018-10-26T09:43:15.512Z"
                    Version="2.0">
    <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">urn:uuid:174033bc-0281-306e-8152-55d343adeac3</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="true"
                        Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:transient"/>
    <saml:Conditions NotBefore="2018-10-26T09:43:15.512Z"
                     NotOnOrAfter="2018-10-26T09:53:15.512Z"/>
    <samlp:Scoping>
        <samlp:IDPList>
            <samlp:IDPEntry
Loc="https://tunnistus.telia.fi/uas/saml2/SingleSignOnService"
                            ProviderID="https://tunnistus.telia.fi/uas"/>
        </samlp:IDPList>
        <samlp:RequesterID>urn:uuid:174033bc-0281-306e-8152-
55d343adeac3</samlp:RequesterID>
    </samlp:Scoping>
</samlp:AuthnRequest>
```

3.3.1 Requested authentication context

Service Provider may specify the authentication method used to authenticate the user. This can be done by passing RequestedAuthnContext element in the authentication request. The following example specifies Mobile ID to be used to authenticate the user.

```
<samlp:RequestedAuthnContext xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
Comparison="exact">

<saml:AuthnContextDeclRef>https://tunnistus.telia.fi/uas/saml2/names/ac/mpki.tel
ia.1</saml:AuthnContextDeclRef>
</samlp:RequestedAuthnContext>
```

The following table lists available authenticated methods and corresponding *RequestedAuthContext* value.

Authentication method	RequestedAuthnContext
Mobile ID	https://tunnistus.telia.fi/uas/saml2/names/ac/mpki.telia.1
Aktia	https://tunnistus.telia.fi/uas/saml2/names/ac/oidc.aktia.1
Ålandsbanken	https://tunnistus.telia.fi/uas/saml2/names/ac/oidc.alandsbanken.1
Danske Bank	https://tunnistus.telia.fi/uas/saml2/names/ac/oidc.danskebank.1
Handelsbanken	https://tunnistus.telia.fi/uas/saml2/names/ac/oidc.handelsbanken.1
Nordea	https://tunnistus.telia.fi/uas/saml2/names/ac/oidc.nordea.1
Oma Säästöpankki	https://tunnistus.telia.fi/uas/saml2/names/ac/oidc.omasp.1
Osuuspankki	https://tunnistus.telia.fi/uas/saml2/names/ac/saml.op.1
POP Pankki	https://tunnistus.telia.fi/uas/saml2/names/ac/oidc.pop.1
Säästöpankki	https://tunnistus.telia.fi/uas/saml2/names/ac/oidc.sp.1
S-Pankki	https://tunnistus.telia.fi/uas/saml2/names/ac/oidc.spankki.1
Hightrust.id	https://tunnistus.telia.fi/uas/saml2/names/ac/oidc.hightrust.id.1

3.4 Authentication response

The assertions that identification broker service creates are standard signed SAML2 WebSSO profile assertions as described in [SAML-Core], [SAML-Bindings], and [SAML-Profiles].

All AuthnStatements created by identification broker service contain the authentication context declaration reference (AuthnContextDeclRef) of the authentication method that was used to authenticate the client at UAS.

Identification broker service may send additional attributes about the user. The assertion will have an attribute statement with a set attributes, each of which may have multiple values. Additional optional user attributes may also be returned, so the customer's implementation should tolerate unexpected user attributes and simply ignore them if they're not found useful.

Name	FriendlyName	Example	Authentication method
urn:oid: 2.5.4.4	`FamilyName`	`Meikäläinen` `von Essen`	BANK ID MOBILE ID

urn:oid:
1.2.246.575.1.14
	`FirstNames`	`Matti Elmeri Valdemar`
		`Anna-Liisa Hilkka`
		(all known current first/given names, space separated)
			BANK ID
			MOBILE ID

urn:oid: 1.3.6.1.5.5.7.9.1	`DateOfBirth`	`1971-06-28` (YYYY-MM-DD)	BANK ID (FI, NO) MOBILE ID (FI) MitID DK

urn:oid:
1.2.246.21
	`HETU`	`220750-999Y`
		`141002A909X`
		(Finnish personal identity code, henkilötunnus) *
			BANK ID (FI)
			MOBILE ID (FI)

http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier	`PersonIdentifier`	`FI/SE/811228-9874`	All Non-Finnish person identifiers

3.4.1 Sample authentication response

```
<samlp:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://service.customer.com/spsso/saml2/AssertionConsumerService"
ID="_0e0b7df6aa47c9f59f7192d03080d7055129e693"
InResponseTo="_487a3cd30d7778d5665b6b13db908d35b8e594bc"
IssueInstant="2018-10-26T09:43:48.772Z"
Version="2.0">
<saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://tunnistus.telia.fi/uas</saml:Issuer>
```

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
/>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha256" />
<ds:Reference URI="#_0e0b7df6aa47c9f59f7192d03080d7055129e693">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"
/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>BV1m3Xg78CcZoH3c4+Z8fl7bKZQ=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
QJxZif8gv5DzhTCfrRLmKR/iBj8cH1S1KWeqJh7G0T4Dl4W7LzXFFbi3JXZYFTPcbA7LWxGa/MJD
p5Mh1jhKiY48H5elFQ/NlcMeqsKJuBkqlY3jK8C/UObtbOILTmHueMs3eMeP9t4vnA5XscZwG2yZ
OznhEFvvwjcovDtBsXMYk3P8rs4r4aSn1YP9izp4sK6q4/9sCu573lhh1Kw8ib1OTcA1tSvI39vB
6aYbaNgkIqQ3x3TQkKMTd0XiFs2FvKCeC1EILDJtWEzFe9CLaS79d6QuwxLv+LM5NS47lO3Yjo9b
DiN+Jjwku30h0dpyBIRmWMVdO//TKxXIppvI5g==
</ds:SignatureValue>
</ds:Signature>
<samlp:Status>
<samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</samlp:Status>
<saml:Assertion ID="_64cf9fbf8e1283212863d0cfc802683f7e44b57b"
IssueInstant="2018-10-26T09:43:48.772Z"
Version="2.0">
<saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://tunnistus.telia.fi/uas</saml:Issuer>
<saml:Subject>
<saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:transient"
NameQualifier="https://tunnistus.telia.fi/uas"
SPNameQualifier="urn:uuid:174033bc-0281-306e-8152-55d343adeac3"
>_e1eba62e8f3ed018c2311615d31d4a15338bb24e</saml:NameID>
<saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData
InResponseTo="_4bddf2d5cec6cbd96a679fc92b8e207e7589c572"
NotOnOrAfter="2018-10-26T09:53:48.772Z"
Recipient="https://service.customer.com/spsso/saml2/AssertionConsumerService"/>
</saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotOnOrAfter="2018-10-26T09:53:48.772Z ">
<saml:AudienceRestriction>
<saml:Audience>urn:uuid:174033bc-0281-306e-8152-55d343adeac3</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2018-10-26T09:43:47.798Z"
SessionIndex="_e2ea6af8a029cdca8163291fb31932337d23a7df"
SessionNotOnOrAfter="2018-10-26T10:43:47.814Z">
<saml:AuthnContext>
<saml:AuthnContextDeclRef>https://tunnistus.telia.fi/uas/saml2/names/ac/mpki.tel
ia.1</saml:AuthnContextDeclRef>
```

```
</saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
<saml:Attribute FriendlyName="SATU"
Name="urn:oid:1.2.246.22"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">11223344D</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute FriendlyName="Gender"
Name="urn:oid:1.2.246.575.1.15"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Male</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute FriendlyName="DateOfBirth"
Name="urn:oid:1.3.6.1.5.5.7.9.1"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string"
>1901-01-01</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute FriendlyName="HETU"
Name="urn:oid:1.2.246.21"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">010101-111A</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute FriendlyName="Subject"
Name="urn:oid:2.5.29.17"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">SERIALNUMBER=11223344D, GIVENNAME=Matti Ilmari,
SURNAME=Meikäläinen, CN=Matti Ilmari Meikäläinen 11223344D</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute FriendlyName="DisplayName"
 Name="urn:oid:2.16.840.1.113730.3.1.241"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Meikäläinen Matti Ilmari </saml:AttributeValue>
</saml:Attribute>
<saml:Attribute FriendlyName="FamilyName"
Name="urn:oid:2.5.4.4"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Meikäläinen</saml:AttributeValue>
</saml:Attribute>
```

```
<saml:Attribute FriendlyName="FirstNames"
 Name="urn:oid:1.2.246.575.1.14"
 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="xs:string">Matti Ilmari</saml:AttributeValue>
 </saml:Attribute>
<saml:Attribute FriendlyName="validuntil"
Name="validuntil"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="xs:string">2023-04-15T09:25:19.000</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute FriendlyName="age"
 Name="age"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">117</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute FriendlyName="lang_locale"
Name="lang_locale"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">fi</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```

4 Version history

Versions	Status	Date	Modified by	Comments
2.22		20.11.2024	Jarmo Koskimaa	Overall refresh of the document. Clarifications about authorization request, corrected parameter “State” to “state”, changes in acr_values table, updated list of test accounts, documentation of signed authentication request, addition of client registration, corrected errors regarding Endpoint locations
2.23		26.11.2024	Jarmo Koskimaa	Added Endpoint address table.
2.24		4.12.2024	Jarmo Koskimaa	Added acr value for Telia MPKI Emulator in Pre-prod.
2.25		17.12.2024	Jarmo Koskimaa	Updated ID token / SAML claims.
2.26		10.2.2025	Jarmo Koskimaa	Signed request object parameters clarification
2.27		18.3.2025	Jarmo Koskimaa	Added service disruption info link
2.28		2.5.2025	Jarmo Koskimaa	Correction to aud value in chapter 2.6.2. Refactor of signed request example.
2.29		6.5.2025	Jarmo Koskimaa	Expiration/UNIX epoch time related refinements.