DIGITALISERINGSSTYRELSEN

NemLog-in

Integration with NemLog-in – Local IdP

Contents

Changelog

Date	Version	Change description	Initials
08-11-2022	0.1	First draft	Nets (TMNYM)
14-11-2022	0.2	Added drawings for pre-production. Replied to DIGST comments.	Nets (TMNYM)
12-12-2022	1.0	Added description on how to select privilege allowing local authenticator assignment. Organisation attribute is no longer required – removed from assertion and description.	Nets (TMNYM)
16-12-2022	1.1	Added common issues section. Changed all references to DT4 to 'pre-production'.	Nets (TMNYM)
26-05-2023	1.2	Added section 11.2.2 and Appendix D to document app-switch behaviour of NemLog-in.	Nets (MDBEC)
14-12-2023	1.3	Updated certificate used in metadata in Appendix-B for Test local IdP for pre-production	Nets (NOSTE)

1 Introduction

This document gives a technical description on how user organisations should integrate their Local IdP with NemLog-in3.

By using a Local IdP the user organisation allows its users to apply the same means of identification to log in to service providers connected to NemLog-in as they use for authentication in their own organisation. This will allow such user organisations to provide simpler and more user-friendly access.

In addition, such organisations may also benefit from a simpler administration of employee identities by automating the registration process using the MitID Erhverv IdM API.

However, to connect a Local IdP to NemLog-in the user organisation must implement the NSIS-standard for the relevant assurance level (Substantial or High) and must be approved by the NSIS Supervisory Board at the Danish Agency for Digital Government. The elaborate process of establishing this and other prerequisites for integrating a Local IdP to NemLog-in is described in detail in [LIG].

1.1 Prerequisites

The reader is expected to be familiar with the most recent version of the OIOSAML 3 profile [OIOSAML3] and the related Local IdP profile [OIOSAMLIdP].

The reader should be familiar with the prerequisites for integration, described in [LIG].

1.2 Intended audience

This document is a technical implementation guide aimed at architects and developers.

1.2.1 Terminology

Term	Description
Identity Provider (IdP)	An Identity Provider (IdP) is a trusted entity that authenticates users and generates authentication assertions or other assertions that vouch for a user's (subject's) identity.
Service Provider	A Service Provider (SP) is an entity that relies on assertions from an Identity Provider (IdP) to authenticate or authorize subjects' actions on its resources.
Broker	A Broker serves as an intermediary between the SP and the IdP, see section **Error! Reference source not found.** below.
Local Identity Provider (IdP)	In NemLog-in3 user organisations are allowed to use their own SAML Identity Provider – a *Local IdP* – when their users authenticate in NemLog-in. Local IdP can only be used with employee identities and requires NSIS compliance by the user organisation. The present document is an integration guide for Local IdPs.
Assertion	Data structure produced by an Identity Provider (SAML authority) or similar regarding an act of authentication. The assertion provides information on the authentication performed by a User,

Term	Description
	attribute information about the User, and/or authorization permissions applying to the User with respect to a specified resource.
Metadata	Service providers and Identity Providers gather the information needed to execute the SAML protocol in so-called metadata XML files. NemLog-in metadata contains: • Entity ID – a unique identifier for the party (SP/IdP) in the federation • Cryptographic keys in the form of X.509 certificates - used for signing and encryption • Protocol endpoints • Attribute profile

2 Identity Provider software

Correct implementation of SAML from scratch is a difficult task that require expertise and a substantial development and testing effort.

We strongly recommend that your integration with NemLog-in makes use of available SAML software, see [LIG] for a list of software.

As described in [OIOSAMLIdP] two different integration profiles (or “Product” types as denoted in MitID Erhverv) are available:

1. An OIOSAML3 model
2. A model adapted for Microsoft AD FS integration

The OIOSAML3 model employs the AuthnRequest structure for passing relevant information to the Local IdP. Microsoft AD FS has more strict requirements and less flexibility, so a specific integration profile has been devised that, for example, makes use of Relay State to convey specific information.

If you are integrating a Microsoft AD FS IdP to NemLog-in, you should use the AD FS integration model, otherwise we recommend that you use the OIOSAML3 model.

3 Architectural overview

Local IdPs supplement the MitID and NemID means of identification available for accessing services connected to the NemLog-in IdP:

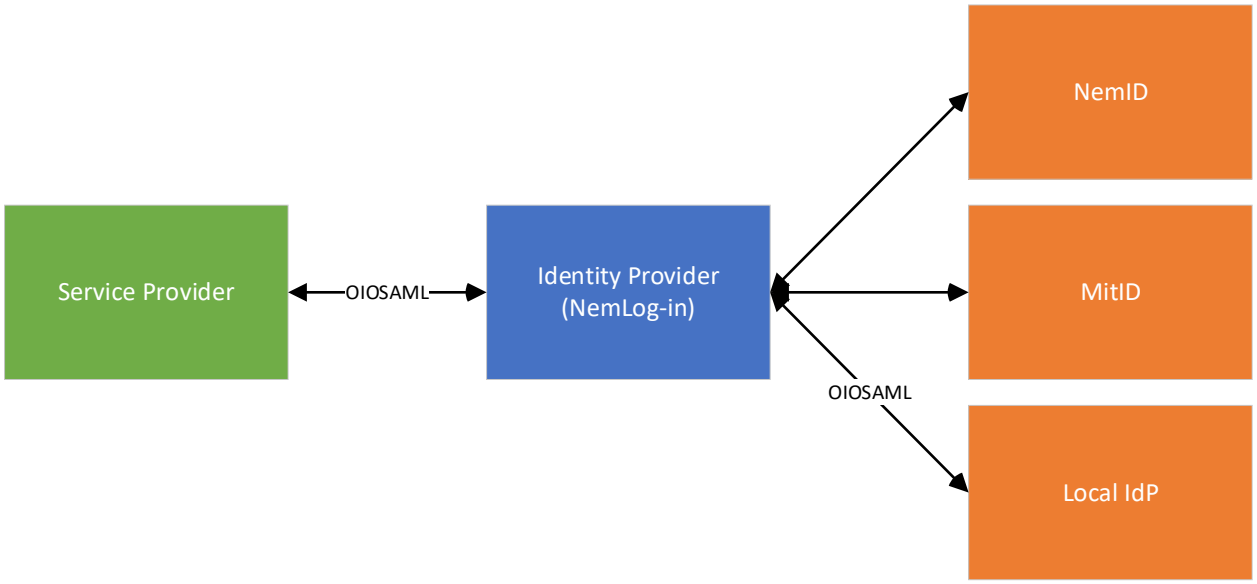


Figure 1: Users in an organisation with a Local IdP may use the same means of identification for accessing both local and public services.

The Local IdP is connected to NemLog-in through a SAML interface, when NemLog-in takes the role of a Service Provider (or Relying Party).

Although NemLog-in supports authentication Brokers to provide access to Service Providers through different integration models,[1] the integration to Local IdPs is always facilitated by the OIOSAML interface to NemLog-in3. The connected Local IdPs therefore only need to support a single Service Provider (NemLog-in) to provide access to all connected services providers connected to NemLog-in to the local IdP users.

An end user may log-in to a Service Provider using local means of identification if two technical conditions are met:

1. The Local IdP must be connected to NemLog-in, i.e. the Local IdP metadata must be registered in MitID Erhverv.
2. The local means of identification must be connected to the MitID Erhverv identity.

The Organisation Administrator is responsible for 1. whereas the Identity Administrator is responsible for 2. If the organisation uses the IdM API for synchronizing the user catalogue with MitID Erhverv, 2. can be performed automatically.

An overview of the features available to NSIS-notified user organisations is given in the table below.

[1] We refer to [NLIB] for details wrt. Broker integration to NemLog-in.

Feature	Availability	Description
MitID Erhverv IdM API	Available for all user organisations, but NSIS-notified organisations have advantages. For example, they may create users which need no further activation steps in MitID Erhverv.	API that allows administration of employee identities. NSIS-notified organisations may create identities and connect local means of identification automatically. Identities are ready to be used immediately. We refer to [NLIDM] for details.
Local IdP connectivity	Only available to NSIS-notified user organisations.	This document.

4 Interaction scenarios

4.1 Simple scenario

The scenario depicted below shows a user logging into a Service Provider with local means of identification.

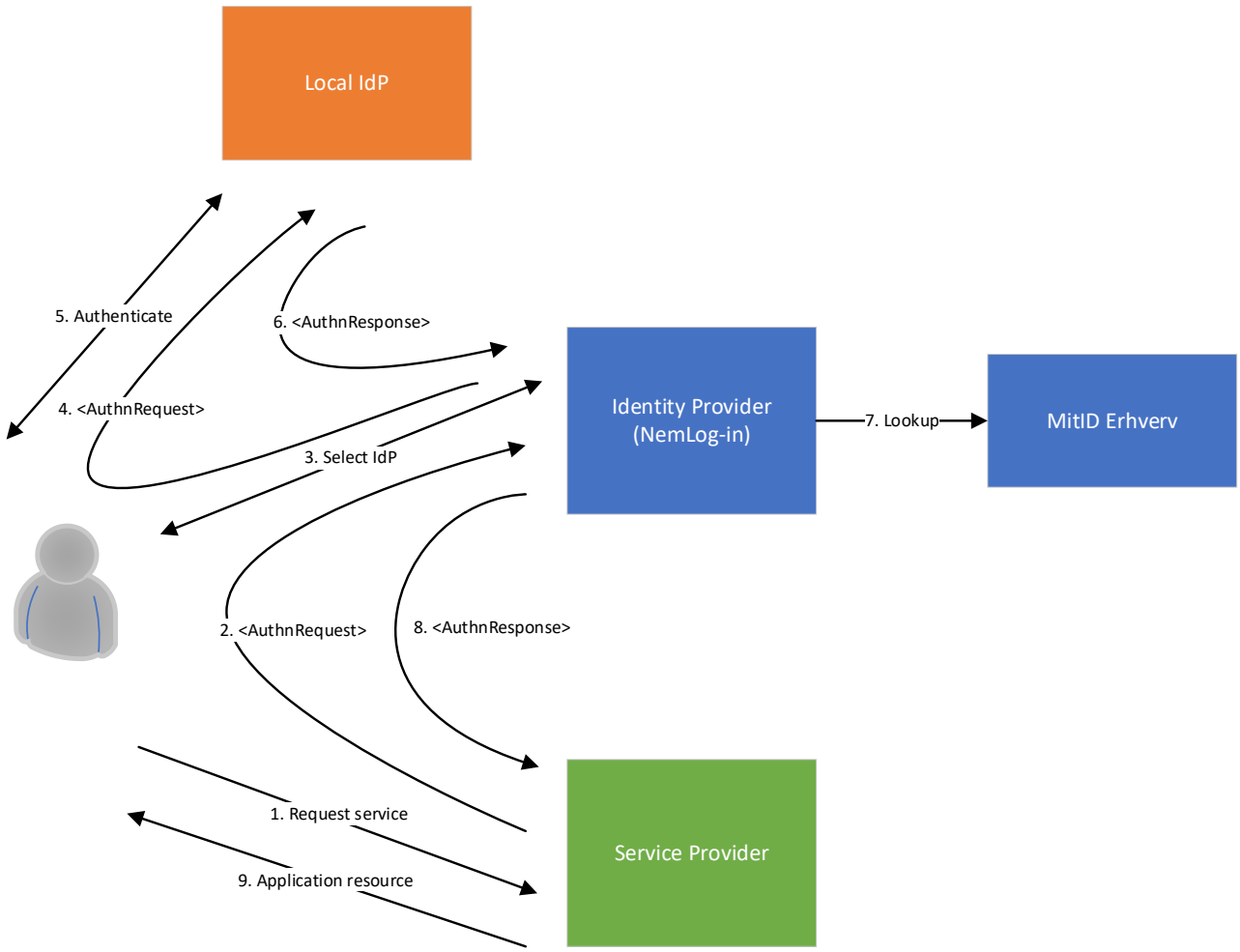


Figure 2: Users logs in using local IdP

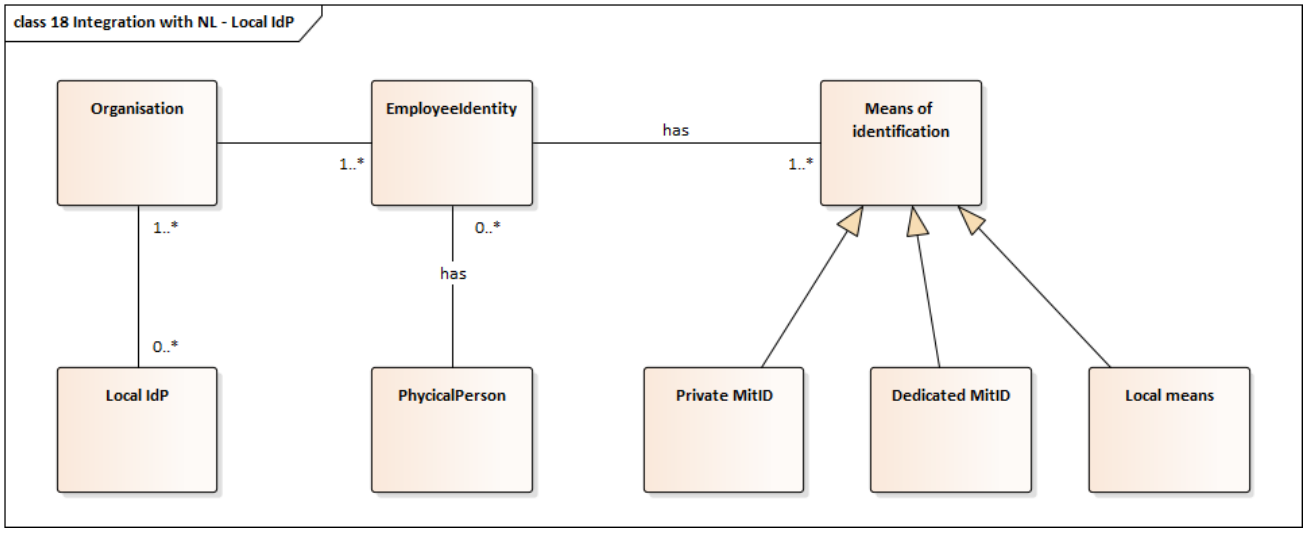
The process is as follows:

1. User accesses a protected resource at Service Provider (SP).
2. Service Provider detects that the user is not logged in, and redirects user to NemLog-in, passing an <AuthnRequest>.
3. User interacts with the NL UI and selects the local IdP of his organisation.
4. NemLog-in redirects the user to the local IdP, passing a second <AuthnRequest> to the local IdP.
5. The local IdP validates the AuthnRequest and determines that the user does not have a session with the local IdP. The local IdP therefore requests the user to perform an authentication using his/her local means of identification.

6. The local IdP validates the resulting authentication response and issues an <AuthnResponse> with an <Assertion>, identifying the local identity and the resulting NSIS level of assurance (LoA) to NemLog-in and redirects the user to NemLog-in.
7. NemLog-in validates the response and the assertion and looks up the associated employee identity in MitID Erhverv by CVR and the local username. NemLog-in retrieves the attributes for that identity requested by the Service Provider (including privileges if SP is public) and builds and signs a new <Assertion>.
8. NemLog-in redirects the user's browser to the Service Provider, passing along an <AuthnResponse> containing the <Assertion> issued in step 7.
9. The Service Provider validates the response and assertion, creates a user-session and grants the user access to the application resource.

5 Data model

The diagram below shows a partial, conceptual data model for MitID Erhverv.



An Organisation may use any number of local IdPs. An EmployeeIdentity ('user') has one or more means of identification. In an organisation with at least one local IdP a given user may be authenticated local means of identification (identified by a username). A consequence is that a given user could use a local IdP for authentication when at work (or on corporate network with VPN) and use his/her private MitID/dedicated MitID in other situations.

A given physical person may posses any number of MitID Erhverv users.

6 Testing integration of a local IdP

6.1 Environments

The following external NemLog-in environments are available:

Environment	Domain name suffix	IdP host name	Test Service Providers
Production	nemlog-in.dk	nemlog-in.mitid.dk	N/A
Integrationtest	test-nemlog-in.dk	test-nemlog-in.pp.mitid.dk	spN.test-nemlog-in.dk
Pre-production, prod-leg	devtest4-nemlog-in.dk	devtest4-nemlog-in.pp.mitid.dk	spN.sp-devtest4-nemlog-in.dk
Pre-production, inttest-leg	**test-devtest4-nemlog-in.dk**	**test-devtest4-nemlog-in.pp.mitid.dk**	**spN-int.sp-devtest4-nemlog-in.dk**

The Integrationtest environment is reserved for the mandatory integration tests that must be performed by service providers and sub-brokers prior to connecting these to Production.

The pre-production environment is a separate environment that provides access to the upcoming release of NemLog-in. The environment is preferred for performing tests as a user organisation. The pre-production environment does not share any data (including test identities) with the Integrationtest environment.

When you create a test-organisation in the pre-production-environment you will have access to MitID Erhverv in both prod-leg (erhvervsadministration.devtest4-nemlog-in.dk) and inttest (erhvervsadministration.test-devtest4-nemlog-in.dk).

If you only wish to perform tests in MitID Erhverv as a user organisation, you may perform the tests in any pre-production leg (prod or inttest) but it is recommended to use the inttest leg. If you also wish to act as a service provider and connect it-systems (SAML Service Provider) to the pre-production environment, you **must** use the inttest-leg for testing since it is not possible to connect it-systems to the pre-production prod-leg. Further, it is only possible to use Service Provider specific test-identities in the inttest-leg.

If in doubt, **use the pre-production, inttest-leg** (highlighted in the table above) for testing local IdP integration. Here you will also have access to the logviewer to inspect NemLog-in error log. [PP]

6.2 Pre-production environment

As described above, the pre-production environment consists of two logical parts (prod- and inttest legs).

The figure below shows a simplistic diagram of the environment. Arrows denote dataflows during registration of services, local IdPs, and identity data.

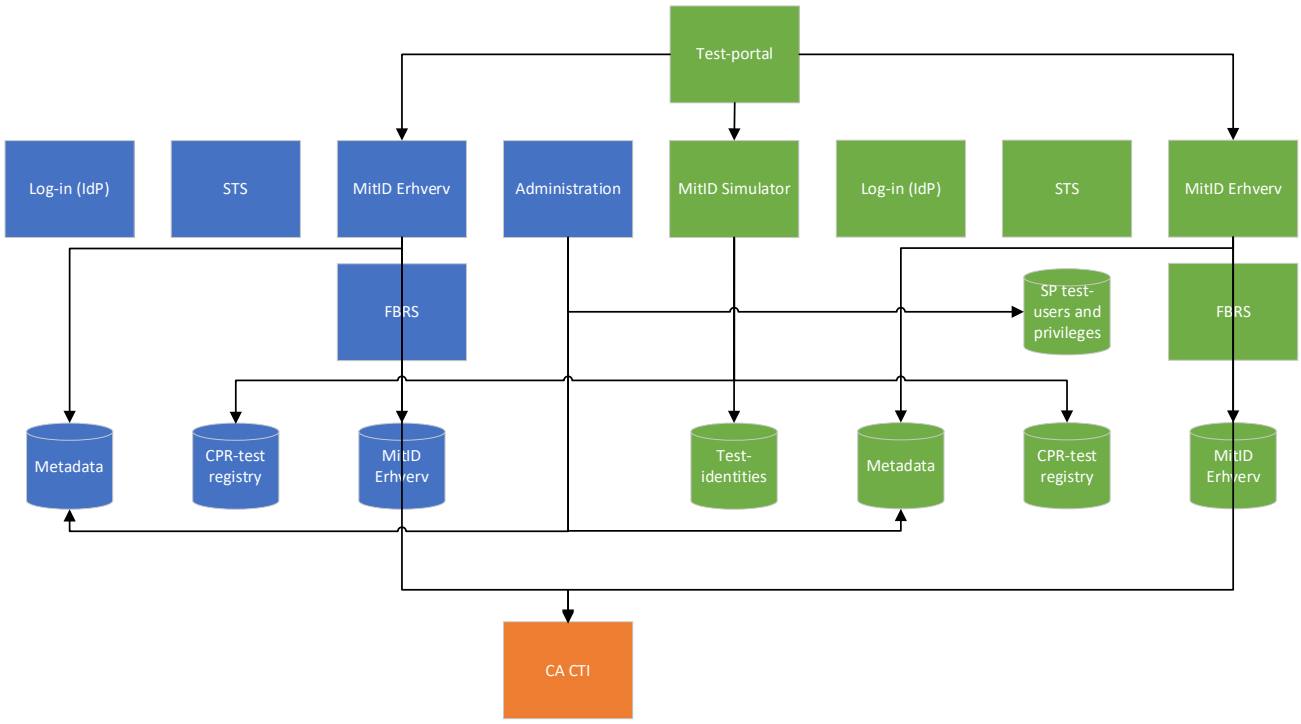


*Figure 3: Pre-production environment with **registration** data flows. Blue shapes belong to prod-leg, green shapes to int-test, and orange shape belongs to CA Customer Test Integration (test-CA) environment.*

The following data flows are depicted:

- Test-portal to MitID Erhverv (both legs) and MitID Simulator: Creating of test organisation, see section 6.3.
- Administration to SP test-users and privileges: Provisioning of service provider test-users.
- Administration to Metadata (both legs): Provisioning of service provider SAML metadata.
- MitID Erhverv to metadata: Provisioning of local IdP metadata.
- MitID Erhverv (both legs) to CA CTI: Registration of certificate data. Both legs utilize the same CA (CTI). CTI CA is also used from the Integrationtest environment.
- MitID Erhverv and FBRS to MitID Erhverv database: Registration of MitID Erhverv users and privileges.
- MitID Simulator to Test-identities: Persisting test-identity data.
- MitID Simulator to CPR-test registry (both legs): Registration of CPR and name information for test-identities.

Authentication data flows are depicted in the figure below.

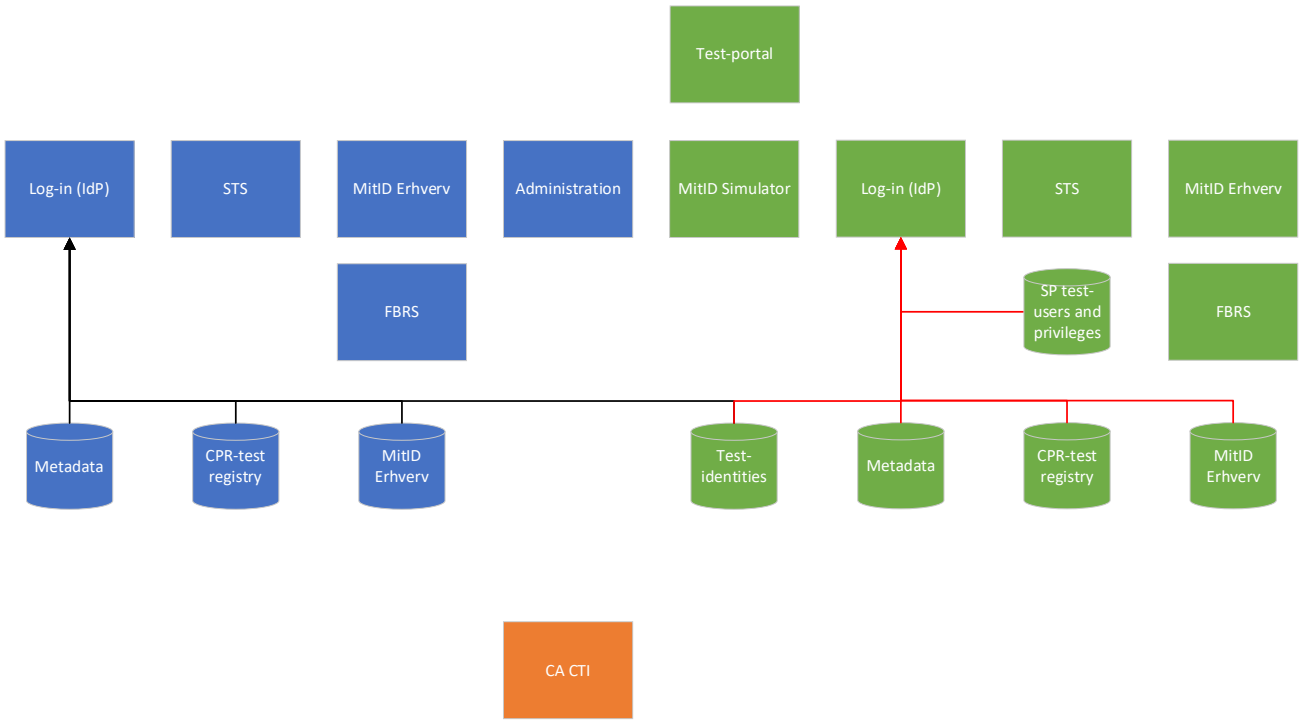


*Figure 4: Pre-production environment with **authentication** data flows. Black arrows: Data flow in prod-leg. Red arrows: Data flow in inttest-leg.*

During authentication, the following data flows are active:

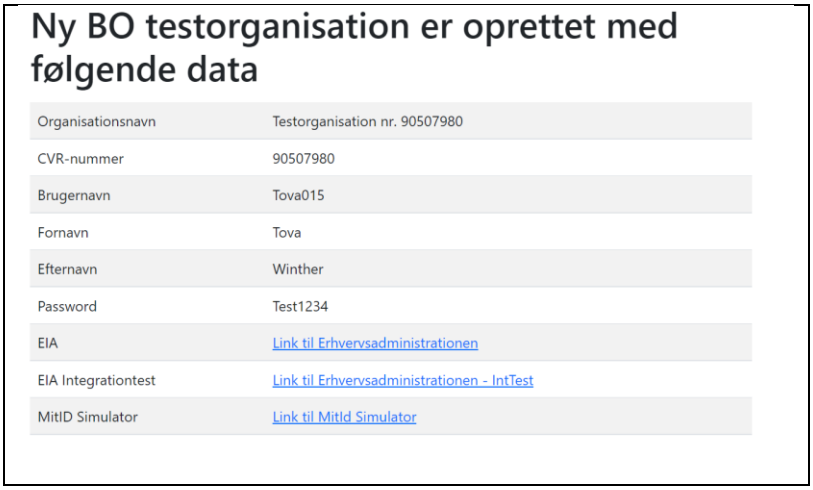
- Metadata to Log-in: Service provider and local IdP metadata used for SAML integration.
- CPR-test registry to Log-in: CPR-test data (first and last names, CPR UUID, etc) used in produced assertions.
- MitID Erhverv to Log-in: User attributes, credential associations, and FBRS privileges.
- SP test-users and privileges to Log-in: Test data for test-users created in Administration by service providers.

6.3 Creating a test organisation

When you are ready to begin integration testing your local IdP you should begin by setting up a test-organisation in the NemLog-in pre-production environment Testportal [PP].

It is important that you indicate the assurance level for the local identification process ("Sikringsniveau for identifikationsproces") to Substantial ("Betydelig") as highlighted above. This will allow connecting a local IdP for the organisation.

This will create a test-organisation with a random name and CVR number, appoint an administrator, and allow you to log-in with a test-identity (here "Tova015") that has the provided password:



The test-identity (Tova015 above) is created in pre-production MitID Simulator [PP].

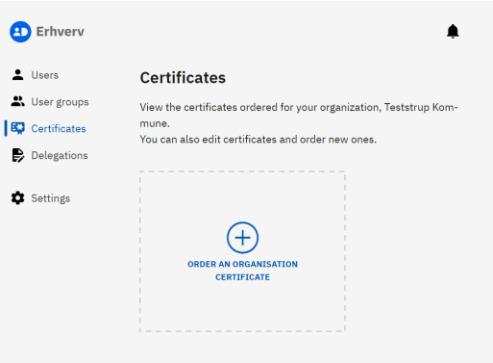
If you need to create a test-organisation with a specific name and CVR number, we refer to section 13.

6.4 Test certificates

When you perform integration tests of a local IdP you will need a test system- or organisation-certificate with a corresponding private key.

These certificates may be issued from MitID Erhverv in the pre-production environment. Note, that both pre-production legs issues certificates from the NemLog-in CTI CA. These certificates are also applicable for use by Service Providers or sub-brokers connecting to Integrationtest.

Navigate to the Certificates menu in MitID Erhverv to issue a certificate.



We refer to [MEUG] for details.

6.5 Common issues

This section describes common issues that you may experience when integrating your local IdP to NemLog-in.

6.5.1 Assertion lifetime

Remember to limit the lifetime of the assertions issued by the local IdP to at most 10 minutes. Otherwise, authentication responses will be rejected by NemLog-in.

6.5.2 Debugging

If NemLog-in displays a generic error message, for example after receiving the authentication response from the local IdP, you may examine the error log by using the LogViewer in the pre-production environment [PP].

7 Connecting a Local IdP

When the NemLog-in Administration ("Forvaltning") has granted local IdP privileges to your organisation, the local IdP can be connected. It is the organisation administrator who has permission to connect your organisation's local IdP.

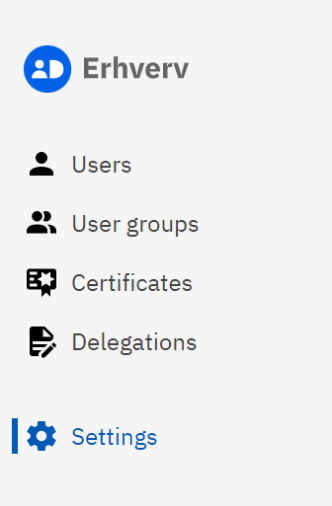
An organisation may use a local IdP in two different ways:

1. The tenant model: The organisation may utilize an IdP connected by another organisation, provided that
    - both organisations are NSIS approved; and
    - the organisation that connected the IdP (the host) and the utilizing organisation (the tenant) agree to share the local IdP.
2. The direct model: An organisation connects its own IdP and does – in terms given above – act as both a IdP host and tenant.

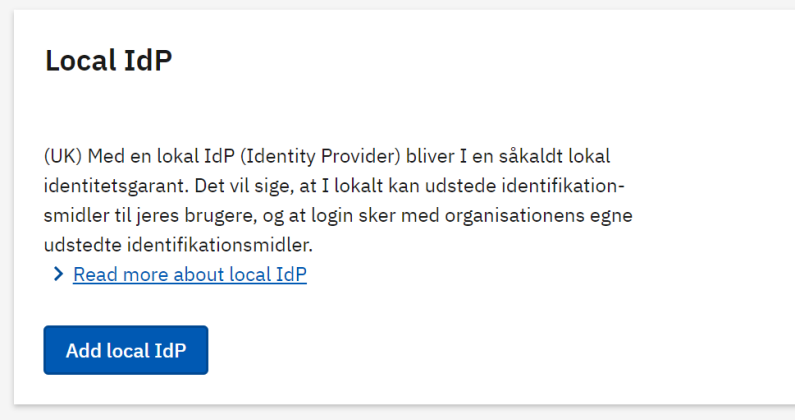
Only organisations that enter the role of hosting an IdP must perform a technical connection of the IdP.

7.1 Technical connection

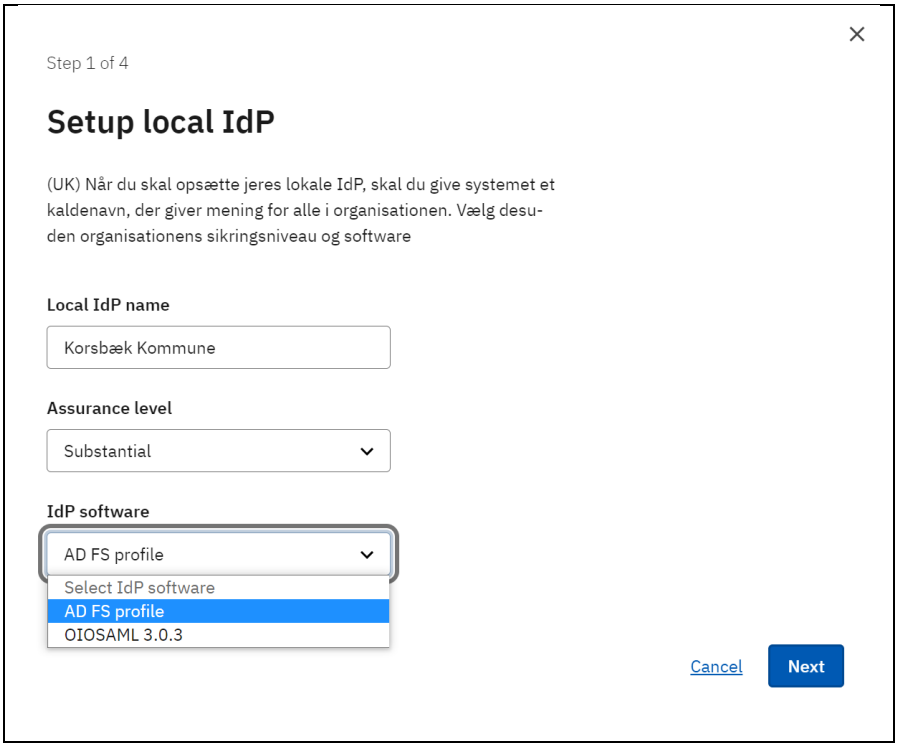
To perform a technical connection of a Local IdP, the organisation administrator must navigate to Settings:



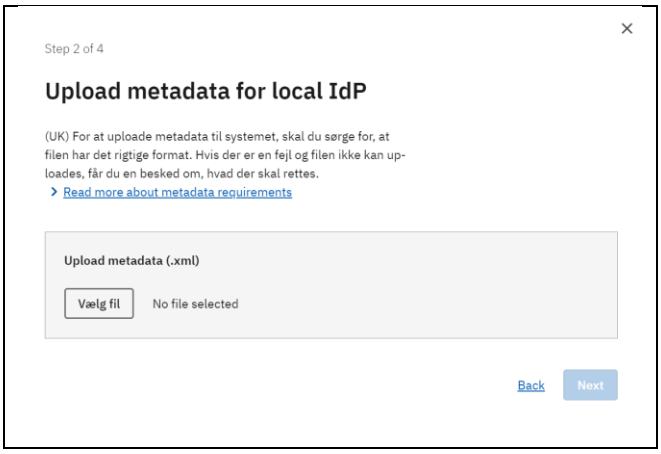
Here, locate the Local IdP section:



And select Add IdP. Now give the IdP a name (this will be presented to end users), choose the assurance level for the IdP (equal to or lower than the NSIS approved assurance level), and select the appropriate integration profile appropriate:

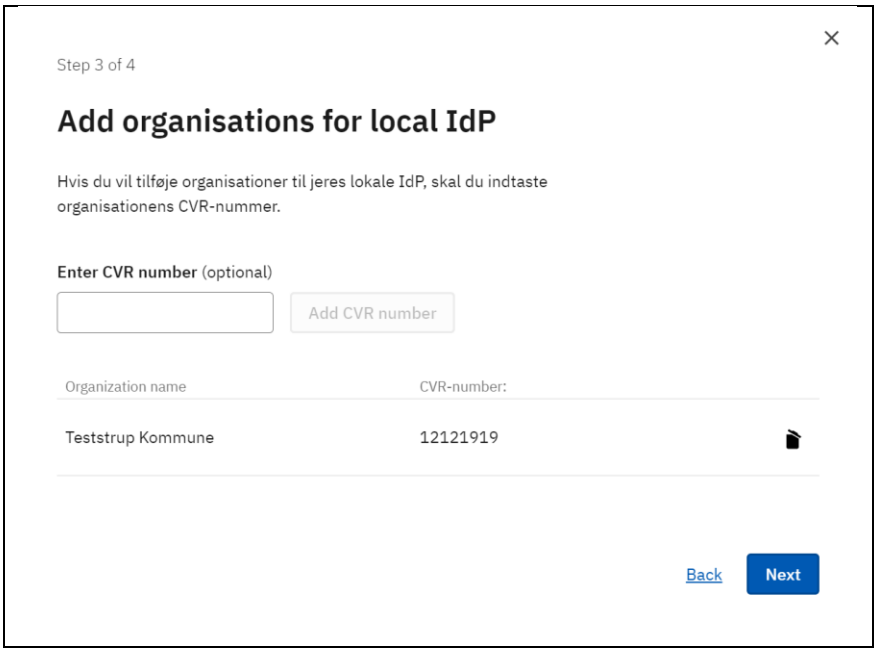


After clicking Next, upload metadata for the local IdP:

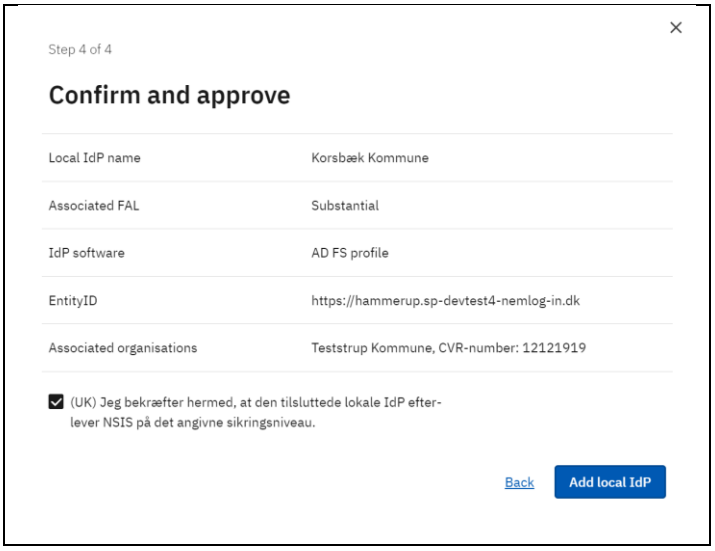


Metadata must conform to [OIOSAML3] – we provide an example in Appendix 2 of this document.

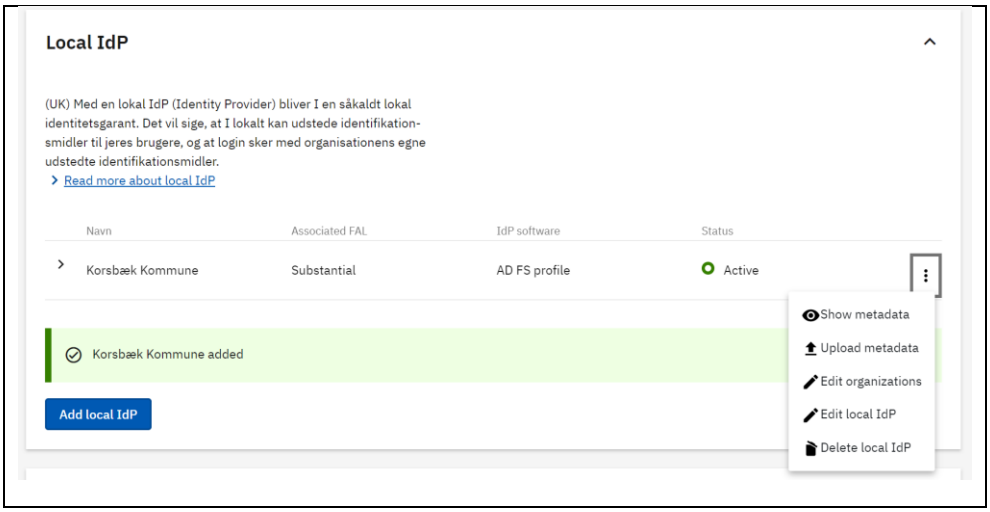
After this, the organisation administrator may choose to add one or more tenants – this step is optional.



Finally, a summary of the settings is shown, and the organisation administrator must confirm, that the IdP he is connecting does in fact comply with the NSIS requirements for that assurance level.



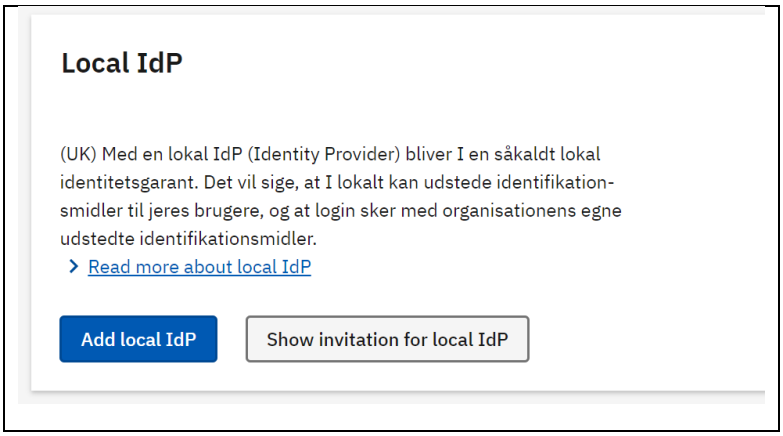
The IdP is now added. The organisation administrator will later be able to alter settings by selecting options in the kebab menu:



7.2 Connecting as tenant

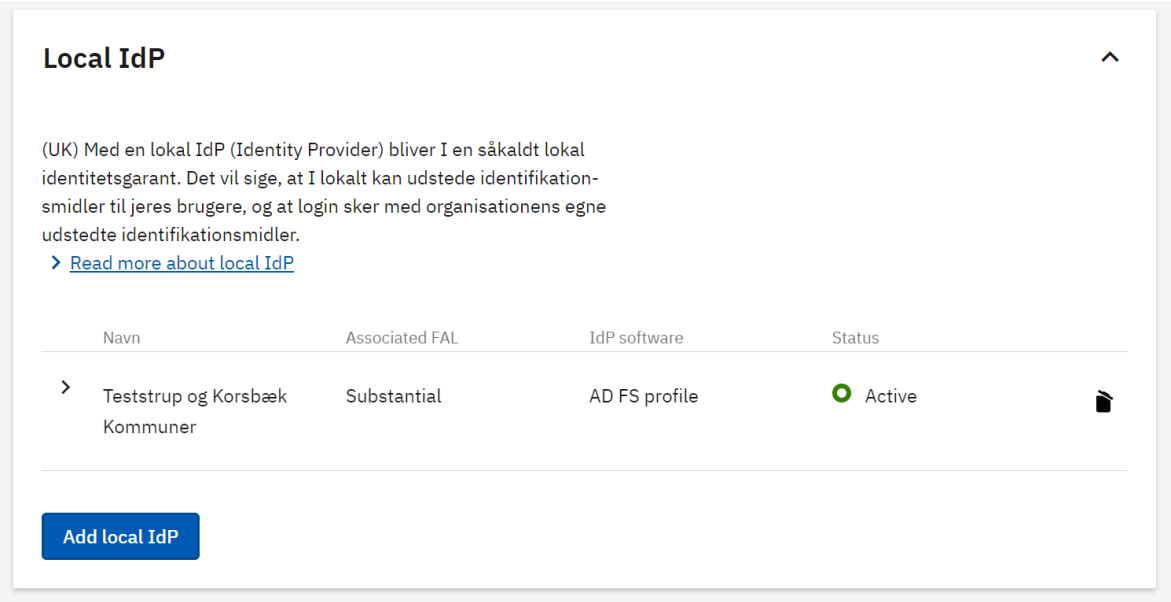
To connect a tenant organisation to a local IdP hosted by another organisation is simple.

When the host organisation has added the tenant organisation to the local IdP, the organisation administrator will note that the option 'Show invitation for local IdP' is available from the Settings menu.



Clicking the button will allow the administrator to confirm to connect:

The administrator may also choose to decline an erroneous invitation. If the invitation is accepted, the local IdP will appear as Active in the section:



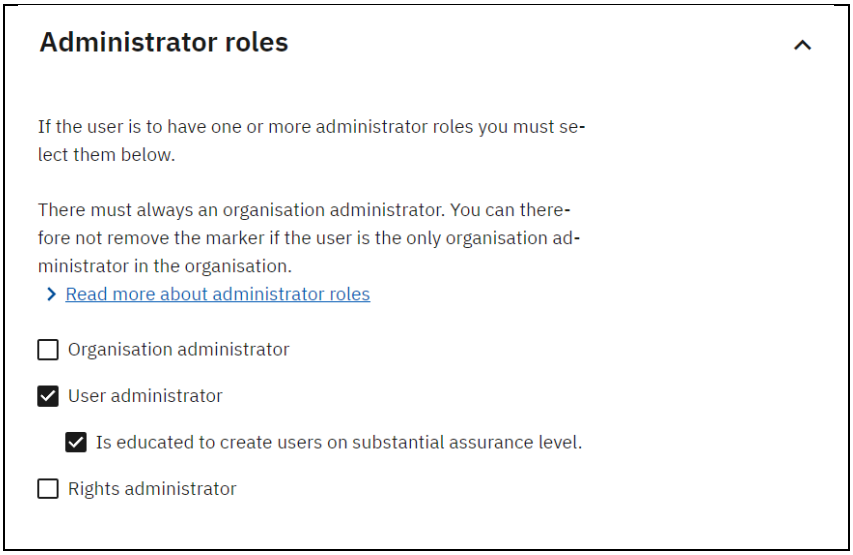
Note, that the only option for the tenant administrator is to disconnect the IdP (trashcan icon) – the tenant administrator is not able to change any settings for the local IdP: The organisation administrator in the hosting organisation may name the local IdP appropriately to convey its intended use to end users.

8 End user authentication

When a local IdP has been connected for the organisation the organisation administrator can allow the organisation to use local means of identification.

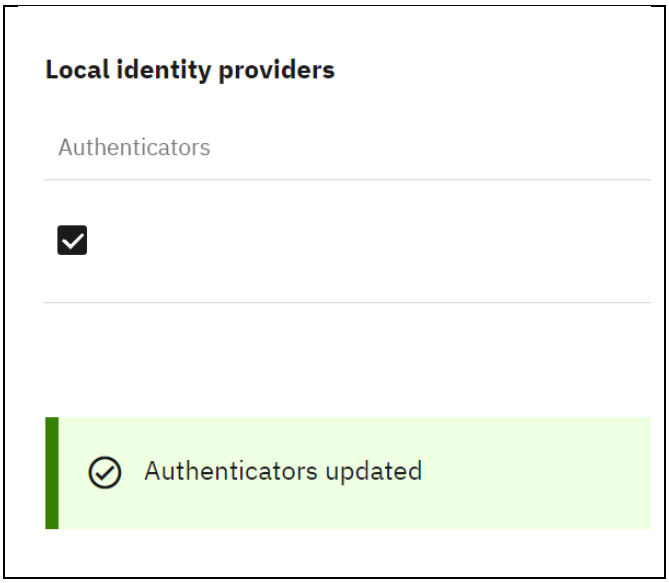
This does, however, require that an additional privilege is assigned to the administrator.

Edit the organisation administrator in MitID Erhverv and open the 'Administrator roles' pane.



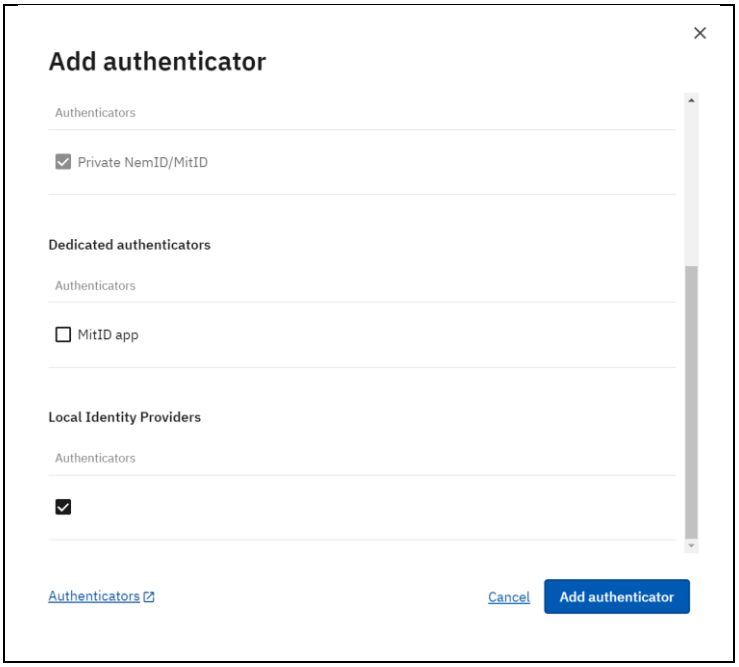
Here the 'Is educated…' privilege must be selected. This indicates that the administrator understands how to perform the NSIS approved (local) identity assurance process appropriately.

With this privilege assigned the administrator may now assign local authenticators to users: Edit the user and in the Authenticators setting section, select 'Authenticators' under 'Local identity providers':

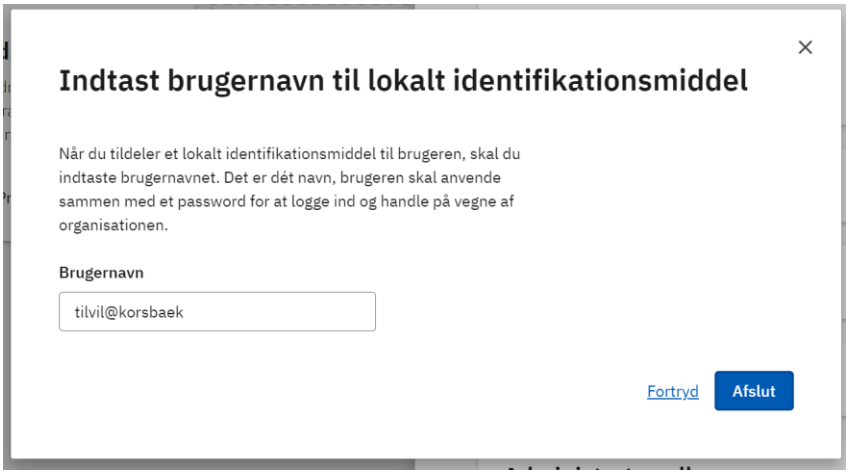


With this in place, the identity administrators may now allow users to log-in using the local IdP. [MEUG]

For active users, simply edit the user and select 'Add authenticator' in the 'Authenticators' ('Identifikationsmidler') section:



And click 'Add authenticator':



Adding local means of identification with the username above, will allow this user to log-in using:

- Any local IdP connected to the organisation; using
- *'tilvil@korsbaek'* as username, i.e. value passed in <Subject><NameID> section of SAML Assertion issued by the Local IdP; and
- the organisation's CVR number passed as OIO SAML https://data.gov.dk/model/core/eid/professional/cvr attribute value.

The username must be unique within the organisation, identified by CVR number.

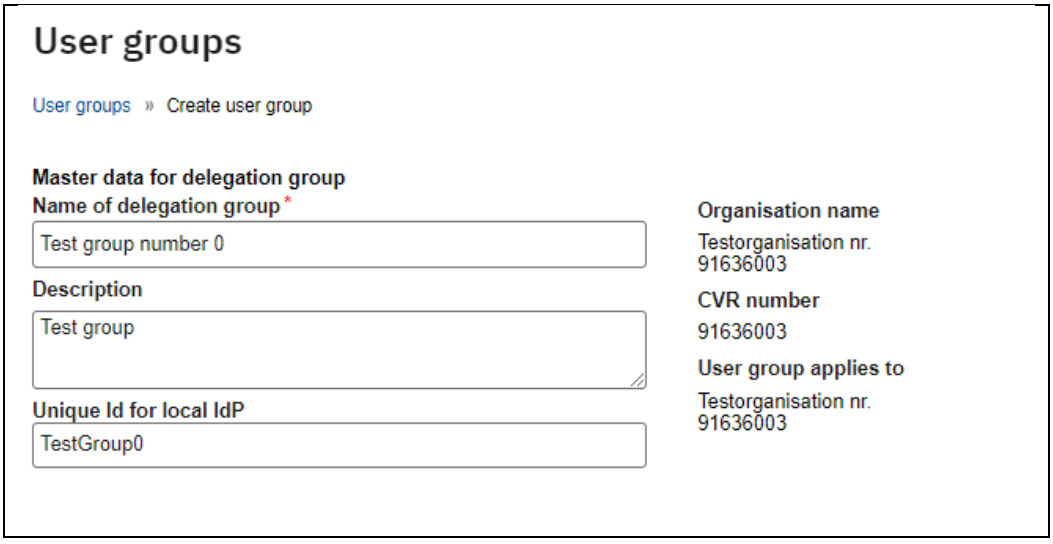
Usernames can also be associated by using the IdM API, we refer to [NLIDM] for details.

8.1 Dynamically assigned group memberships

With a local IdP your organisation will be able to appoint members of specific MitID Erhverv/FBRS rights groups without having to specifically having the rights administrator assign membership using the MitID Erhverv UI or the IdM API.

Instead, group memberships are included as information in the assertion issued by the local IdP, where group memberships are listed in the privileges attribute (https://data.gov.dk/model/core/eid/privilegesIntermediate). This mechanism allows the user organisation to control membership by of these groups by – for example – use of local group memberships (such as Active Directory groups or similar).

To prepare a MitID Erhverv group for this dynamic member assignment, the group must be assigned a unique ID that is used by the local IdP to refer the group. This ID is assigned by the rights administrator in MitID Erhverv (or by using the IdM API):



The user organisation can now dynamically appoint membership of this group by adding a PrivilegesIntermediate attribute to the issued assertion containing Base64 encoded UTF-8 bytes of a privileges assignment according to [BPP]. The value must conform to the syntax described in [BPP] but with different semantics since the XML structure is only used to hold a list of group IDs.

As an example, a user in the organisation with CVR 91636003 would be appointed as member of groups with ids 'TestGroup0' and 'TestGroup1' in the established session by the following BPP structure:

```
<?xml version="1.0" encoding="UTF-8"?>
<bpp:PrivilegeList xmlns:bpp="http://digst.dk/oiosaml/basic_privilege_profile"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >
    <PrivilegeGroup Scope="urn:dk:gov:saml:cvrNumberIdentifier:91636003">
        <Privilege>TestGroup0</Privilege>
        <Privilege>TestGroup1</Privilege>
    </PrivilegeGroup>
</bpp:PrivilegeList>
```

NemLog-in will – after receiving such an assertion – assign relevant privileges from the groups to the Service Provider requesting log-in. Other Service Providers participating in the same SSO session will also receive relevant privileges.

Note, that the local IdP is not allowed to send actual privileges understood by NemLog-in Service Providers. The only allowed form of PrivilegesIntermediate allowed to be sent by local IdPs is that above, exhibiting the following properties:

- <PrivilegeList> must contain a single <PrivilegeGroup> element
- The <PrivilegeGroup> must have a Scope attribute, scoping the group to the same CVR number as passed in the CVR number attribute.
- The <PrivilegeGroup> element must contain at least one <Privilege> element
- The value of <Privilege> elements must be a 'Unique ID for local IdP' for a MitID Erhverv user group.

9 Authentication with test-IdP

There are two test-IdPs installed in the pre-production environment. These are primarily used for internal testing but can also be used by external parties who wish to inspect the log-in and log-out flows, message contents etc.

This section describes how this is achieved.

9.1 Location of test-IdPs

The two inttest-leg instances are available at:

- https://testlocalidp0-int.sp-devtest4-nemlog-in.dk
- https://testlocalidp1-int.sp-devtest4-nemlog-in.dk

and the prod-leg instances at:

- https://testlocalidp0.sp-devtest4-nemlog-in.dk
- https://testlocalidp1.sp-devtest4-nemlog-in.dk

Metadata for the inttest instances are provides in Appendix B.

9.2 Connecting test-IdP to test-organisation

You connect the test-IdPs just like any other local IdP, as described in section 7.

But first you need to prepare the metadata file to use. Begin by using the metadata file for the test-IdP you wish to use given in Appendix B.

Now select an EntityID that you wish to use for the test-IdP in your test organisation setup. Replace the EntityID attribute value in the EntityDescriptor element with that chosen EntityID. Remember, that the EntityID – although is has the syntax of a URL – is merely a name for the IdP; no traffic is sent to the EntityID URL and no response is expected if you attempt to “access” the EntityID URL.

For example:

```
entityID="https://testlocalidp0-int.sp-devtest4-nemlog-in.dk"
```

becomes

```
entityID="https://idp.korsbaek.dk"
```

Note, that the EntityID must have prefix ‘http://’ or ‘https://’.

This is the only change required. Now you can connect the test-IdP as described in section 7.

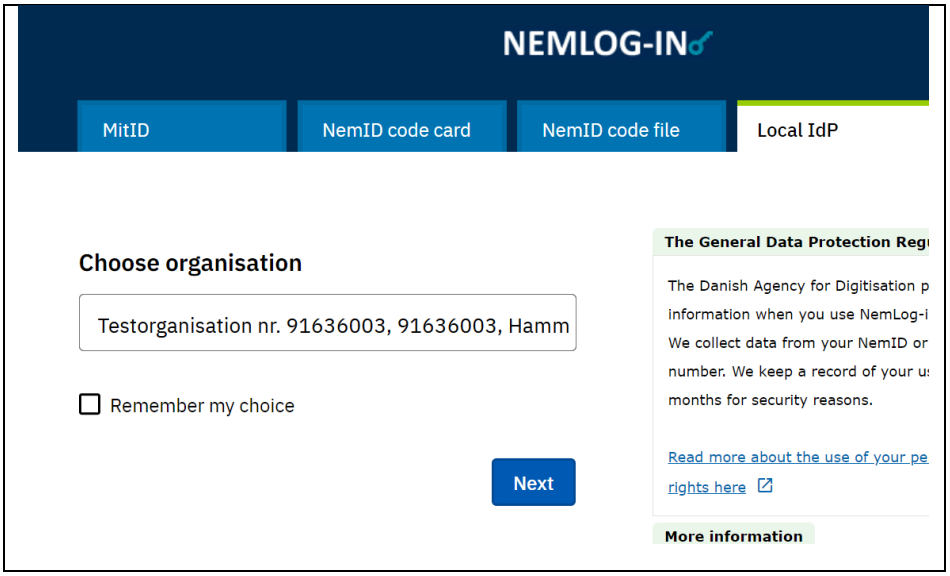
9.3 Authentication with the test-IdP

With the test-IdP connected to your test organisation, you are ready to perform authentications.

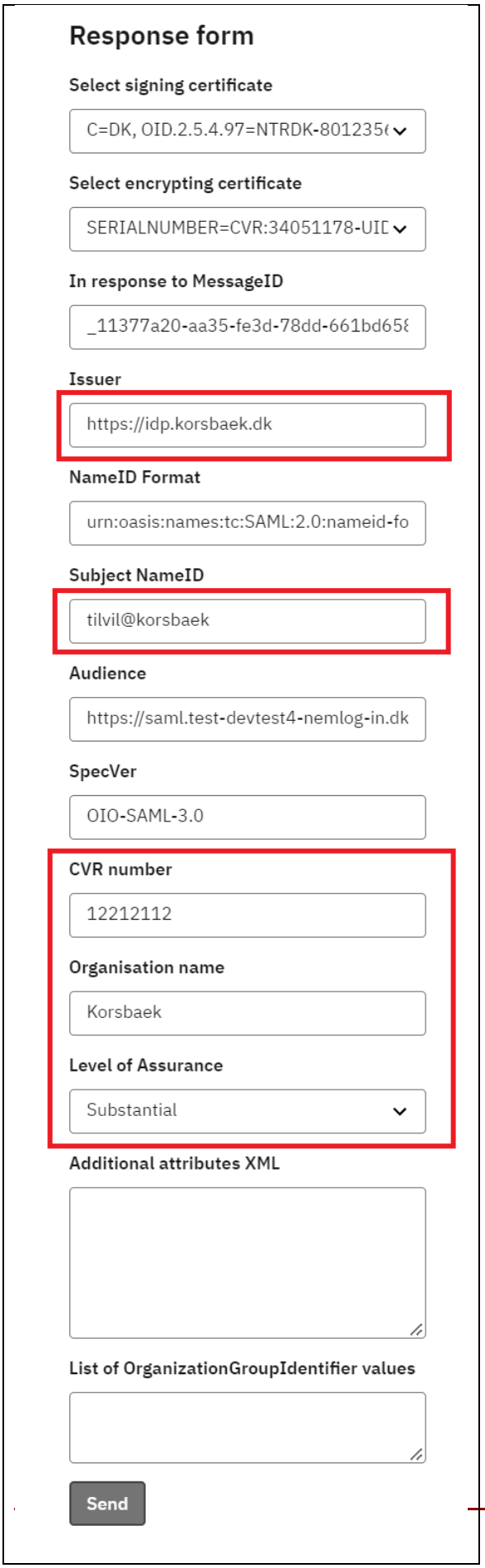
You can use the test-services that are available in the environment [PP], here we will use test service 3, at https://sp3-int.sp-devtest4-nemlog-in.dk/.

The test service is also an internal testing tool and has a lot of different options. For a simple test, it suffices to simply click “Login” in the lower left corner.

You will be redirected to NemLog-in, where you must select the 'Local IdP' pane, search for and the connected IdP, and click Next.



You will then be redirected to the test-IdP. The top of the screen will display elaborate information about the authentication request, and the bottom will show a Response form, that you must fill out to allow the IdP to create and assertion for NemLog-in. Note, that the test-IdP does not perform any authentication as it is only used for test-purposes.


Response form
Select signing certificate
C=DK, OID.2.5.4.97=NTRDK-801235(
Select encrypting certificate
SERIALNUMBER=CVR:34051178-UID
In response to MessageID
_11377a20-aa35-fe3d-78dd-661bd65
Issuer
https://idp.korsbaek.dk
NameID Format
urn:oasis:names:tc:SAML:2.0:nameid-fo
Subject NameID
tilvil@korsbaek
Audience
https://saml.test-devtest4-nemlog-in.dk
SpecVer
OIO-SAML-3.0
CVR number
12212112
Organisation name
Korsbaek
Level of Assurance
Substantial
Additional attributes XML
List of OrganizationGroupIdentifier values
Send

ID:18

You need to fill out the following information that will enter the issued assertion:

- **Issuer:** Replace the default EntityID with the EntityID you provided for the IdP in the uploaded metadata.
- **Subject NameID:** Supply the registered username for the employee identity you wish to authenticate.
- **CVR number:** CVR number for the test organisation.
- **Level of assurance**: LoA for the authentication.

Clicking Send will redirect your browser back to NemLog-in with a SAML AuthnResponse with a signed assertion from the test-IdP. NemLog-in will lookup attributes for the user with the provided Subject NameID (username), issue an assertion for the requesting service provider, and perform another browser redirect back to the service provider.

The test service will then establish a session and allow you to inspect the assertion, including attributes. Note, that neither the assertion issued by the test-IdP nor any of its attributes are forwarded to the service provider. The assertion received by the service provider an created in its entirety by NemLog-in.

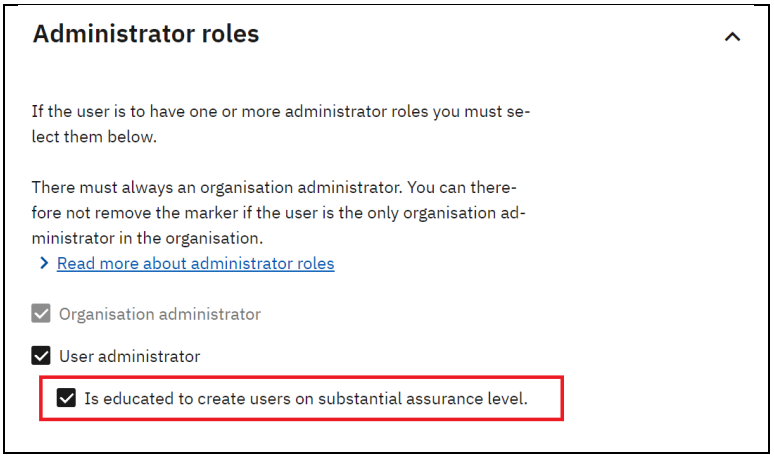
10 Signing

Employees in organisations with local IdP may approve organisational signatures or sealing using the local IdP.

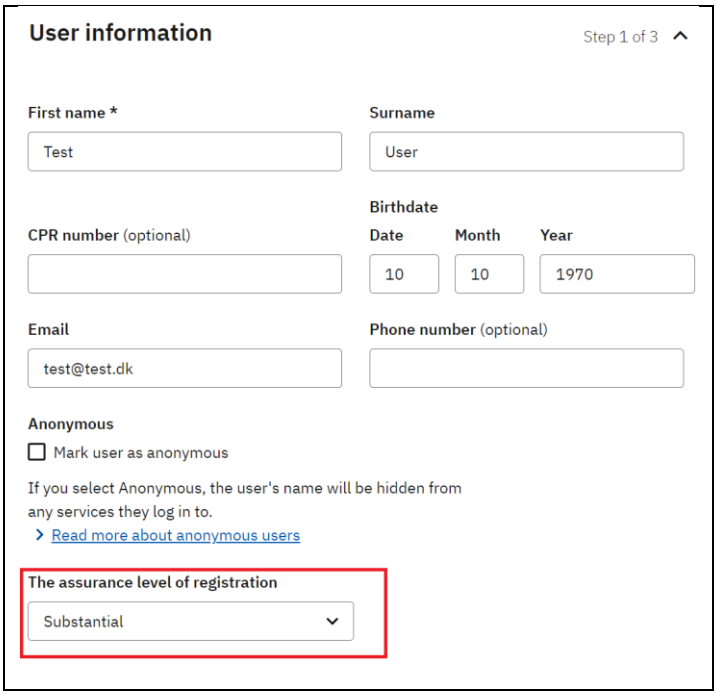
However, only users that have had their identity proven in MitID Erhverv in an activation process where their private MitID has been used, may use a local IdP for signing operations.

10.1 Immediately active users

User organisations that are NSIS-approved have the option of activating users directly with registered assurance level up to their NSIS approval level (usually Substantial) – so called 'immediately active users'. This requires either use of the IdM API or that registration is performed by an identity administrator who has been assigned this privilege by the organisation administrator:



User administrators with this privilege is denoted 'NSIS-privileged user administrators'. NSIS-privileged user administrators may create immediately active users be setting an assurance level of registration ('registered IAL') as shown below:



As mentioned, end users registered directly on Substantial (or higher) do not have to activate their identity in MitID Erhverv but are - on the other hand - not allowed to perform signing operations since the (in that case) purely local registration process does not conform to all requirements for issuing qualified certificates which occurs when a document is signed.

10.2 Signing with local means of identification

Since users that must be able to perform signing operations must be activated with private MitID such users must be created as described below:

1. Identity administrator: Create the user:
    a. Set assurance level of registration to 'Low' (only for NSIS-privileged identity administrators, plain identity administrators will not have this option).
    b. Assign MitID means of identification to be used, private or dedicated.
    c. Assign local means of identification (username)
2. User: Receives e-mail and follows activation link
3. User: Activates identity and presents private MitID

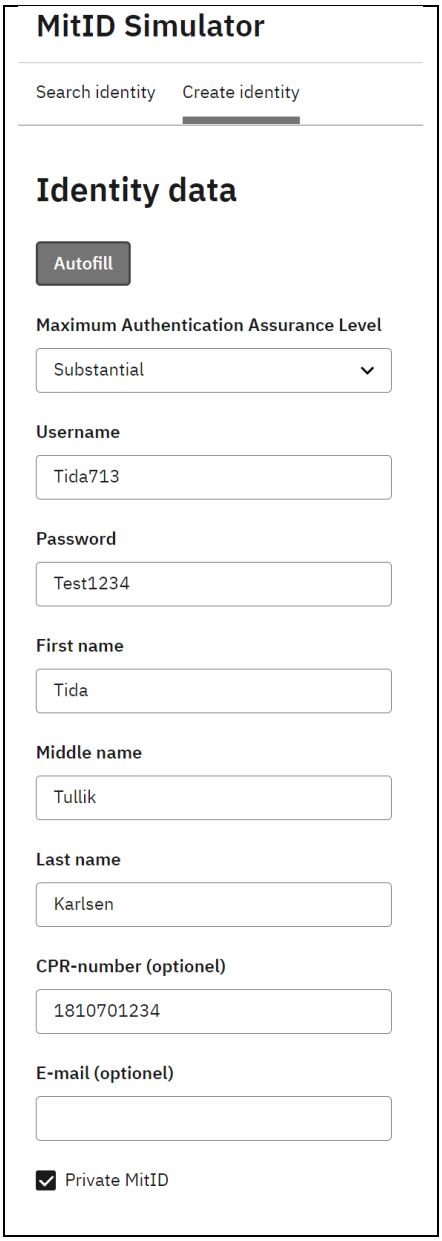
When the user has been activated the identity may be used for approving employee signatures and – if allowed by the organisation – organisation sealing.

10.3 Emulating signature approval

If you wish to test signature approval but do not have a service that uses signing you can emulate a signature flow by using the test-service available in [PP].

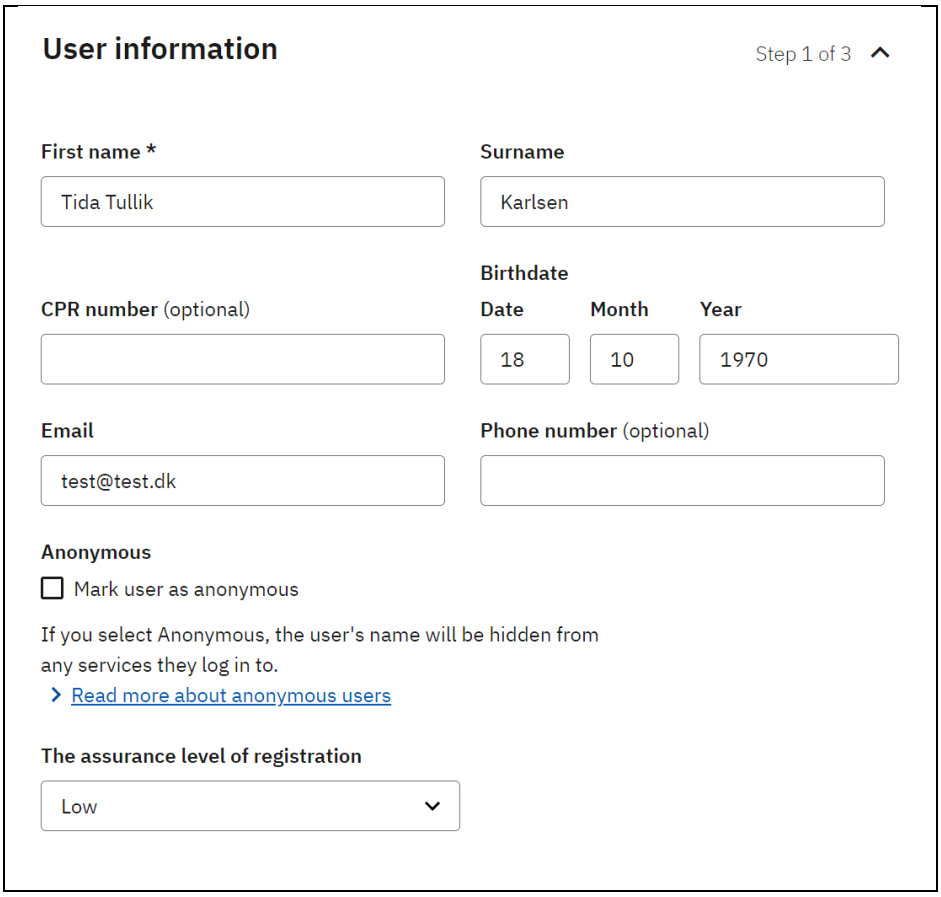
Begin by creating a test-user to use for signing. In the pre-production environment, the process described in 10.2 must be preceded by creating the private identity for which the employee identity is to be created.

This is done in the MitID Simulator [PP]:



It is important that you mark the identity to be private and assign a fictitious CPR number.

Now create the user using the same name and date of birth:

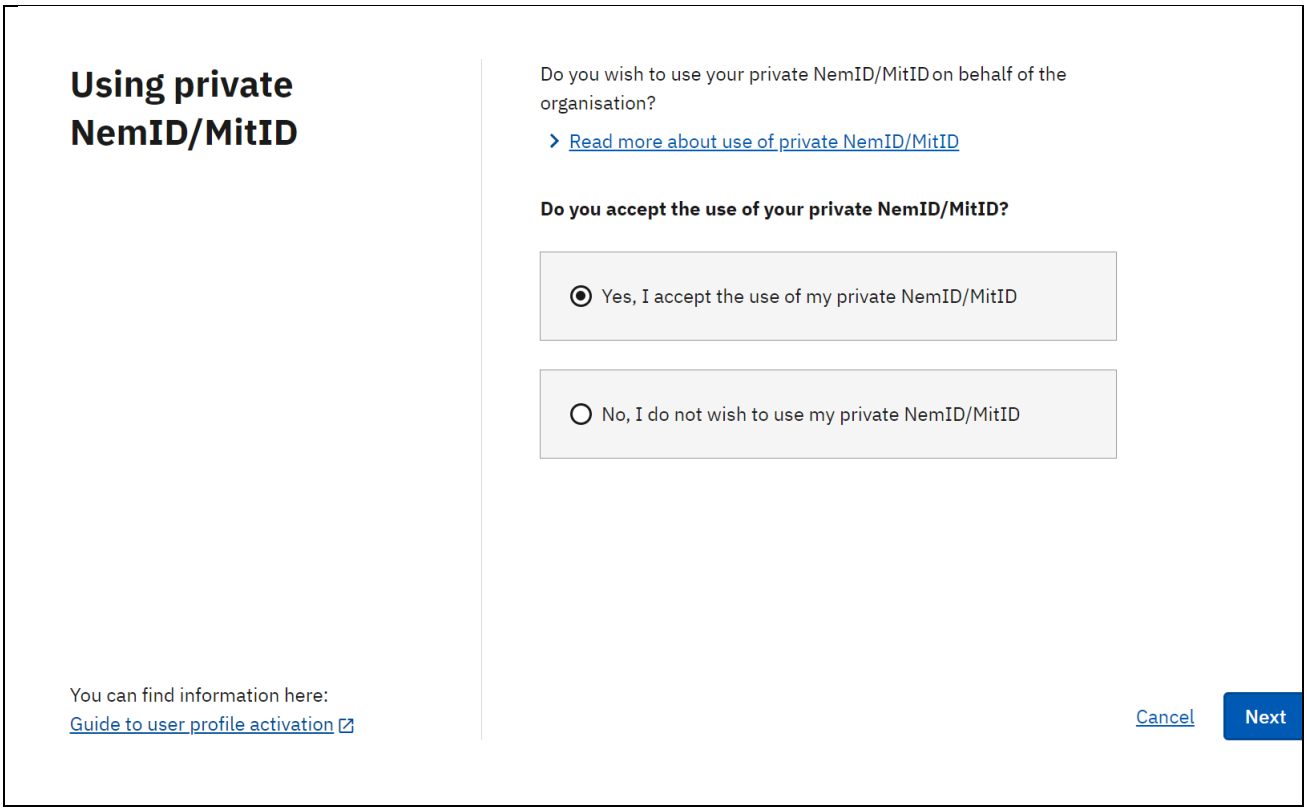


And assign authenticators:

- Private MitID
- Local IdP (username)

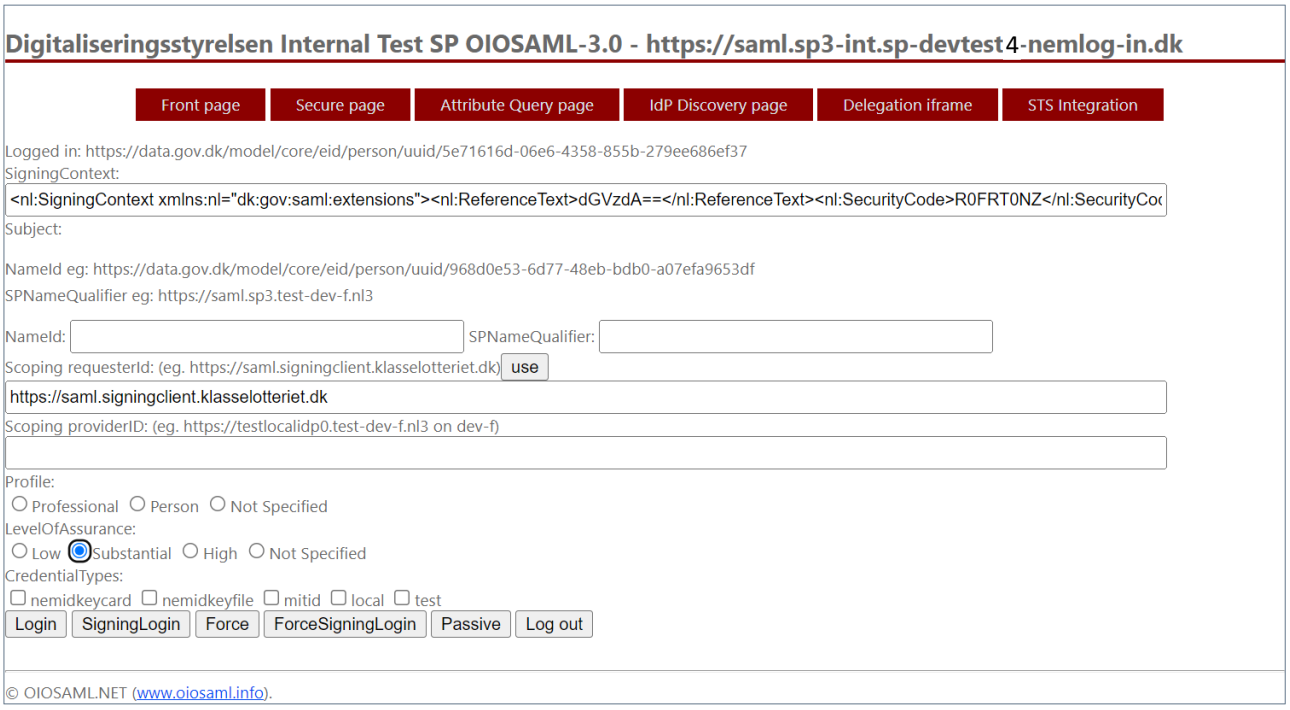
When completed, make note of the activation code.

Now click the activation link in the received email and accept the use of private MitID:



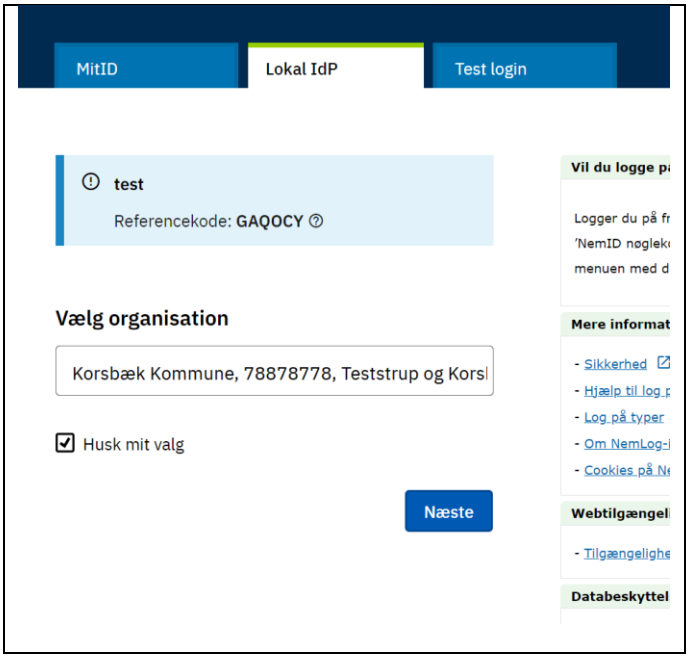
Next, enter the noted activation code – and the user is activated.

Now the signature flow can be emulated using the test-service [PP]:



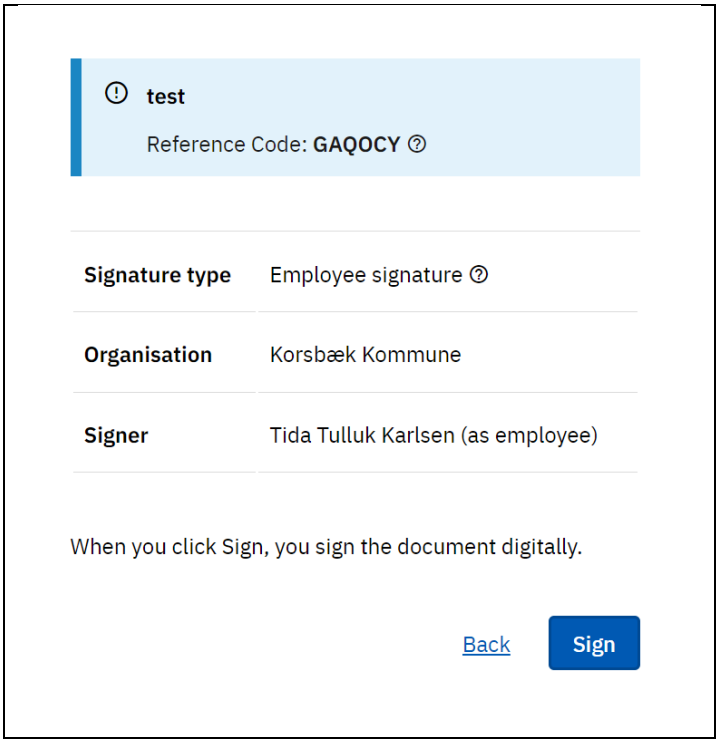
- Click ‘Use’ to add a requesterID.
- Select Substantial.

- Click 'ForceSigningLogin'.



Now select the appropriate IdP and provide input in the test-IdP as described in section 9 above.

After accepting the terms for signing you will see the receipt page:



When you click sign you will be allowed to inspect the contents of the special assertion issued during signing. If no error messages are shown the signing flow is completed successfully.

11 Technical requirements

11.1 Metadata

The organisation administrator supplies metadata for the local IdP. Metadata is uploaded in MitID Erhverv when the IdP is registered as described in section 7.

Metadata requirements are the same, regardless of the chosen integration profile (OIOSAML3 or AD FS).

11.1.1 EntityID

Metadata must conform to [OIOSAMLIdP]. Note that

- the chosen EntityID must have prefix 'https://' or 'http://' – generalization of [OIO-GE-03] – and;
- multiple signing certificates are supported [OIO-IDP-41]

11.1.2 Subject NameID formats

The metadata must reflect the local IdP chosen Subject NameID format amongst the five formats supported by NemLog-in:

- urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
- urn:oasis:names:tc:SAML:2.0:nameid-format:Kerberos
- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName
- urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName

11.1.3 SAML Single Sign on support

NemLog-in only supports SAML HTTP redirect binding for transmitting authentication requests to local IdPs. (<SingleSignOnService> element in metadata).

11.1.4 SAML Single Logout support

NemLog-in supports both SAML HTTP redirect and POST bindings for transmitting logout requests to local IdP (<SingleLogoutService> element in metadata).

11.2 Authentication requests

NemLog-in requests authentication at the local IdP by forwarding an AuthnRequest using SAML HTTP redirect binding. This is the only binding supported for local IdPs.

The authentication request conforms to [OIOSAMLIdP] and convey the following information to the local IdP:

- Desired NSIS assurance level [OIO-SP-06]
- Desired attribute profile [OIO-SP-07] (always 'https://data.gov.dk/eid/Professional')

Identifiers in [OIO-SP-06] refer to requirements in [OIOSAMLIdP].

The authentication request conforms to the previous version of [OIOSAMLIdP] v1.0.2 wrt. the following:

- EntityID of requesting Service Provider as <RequesterID> element [OIO-SP-09]

Note, that this behaviour is replaced in [OIOSAMLIdP] by the optional [OIO-SP-09] (ProviderName) which is **not** currently implemented by NemLog-in.

You may use the test-IdPs to inspect <AuthnRequests> as described in section 9.

11.2.1 AD FS profile specifics

When the local IdP uses the AD FS integration profile the data described in section 11.2 above is included in the RelayState request parameter.

The contents of the <RequestedAuthnContext> element contains an AD FS specific <AuthnContextClassRef> requesting multi-factor authentication as shown below:

```
<RequestedAuthnContext comparison="exact">
    <AuthnContextClassRef
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://schemas.microsoft.com/claims/multipleauthn</AuthnContex
tClassRef>
  </RequestedAuthnContext>
```

11.2.2 Mobile app-switch

NemLog-in will communicate mobile app-switch information it receives from its service provider to enable local IdPs to make automatic return app-switch when authentication at the local IdP requires another app as part of the authentication process. The app-switch behaviour is designed to target support for mobile app-switch using either Dynamic Links on Android [DynLinks] or Universal Links on iOS [UniLinks].

The necessary information will be communicated using SAML Extension named AppSwitch in the AuthnRequest. The AppSwitch element contains the platform (Android or iOS) and the return URL for the address of the app which the authenticator app should return the end user to after is done in the authenticator app. The AppSwitch XML element takes the form as shown in example below.

```
<nl:AppSwitch xmlns:nl="https://data.gov.dk/eid/saml/extensions">
    <nl:Platform>Android</nl:Platform>
    <nl:ReturnURL>dk.serviceprovider.test</nl:ReturnURL>
</nl:AppSwitch>
```

A complete SAML AuthnRequest with the AppSwitch extension will take the form as shown in the example below.

```
<?xml version="1.0"?>
<samlp:AuthnRequest
    ID="id9eb5dd256c25461584a2796994feab1d"
    ...
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer>https://saml.test-devtest4-nemlog-in.dk</saml:Issuer>
  <samlp:Extensions>
    <nl:AppSwitch xmlns:nl="https://data.gov.dk/eid/saml/extensions">
      <nl:Platform>Android</nl:Platform>
      <nl:ReturnURL>dk.serviceprovider.test</nl:ReturnURL>
    </nl:AppSwitch>
  </samlp:Extensions>
  ...
</samlp:AuthnRequest>
```

An XML schema for validation of the AppSwitch-element SAML extension can be found in Appendix D.

When using the AD FS integration profile, the app-switch information will be communicated as part of the RelayState request parameter. The following JSON syntax is used.

```
{
  "AppSwitch": {
    "Platform": "Android",
    "ReturnURL": "dk.serviceprovider.test"
```

```
  }
}
```

Note that the JSON structure is also use for [OIO-SP-06], [OIO-SP-07] and [OIO-SP-09] of [OIOSAMLIdP] cf. section 11.2 and therefore the content is delivered as a Base64 encoding of the UTF-8 bytes.

12 References

Most documentation is available here: https://migrering.nemlog-in.dk/nemlog-in-broker/test-og-dokumentation/.

Reference	Description
[LIG]	Guide til implementering af lokal IdP v. 1.1. https://www.mitid-erhverv.dk/avanceret/lokal-idp/
[OIOSAML3]	https://digst.dk/it-loesninger/standarder/oiosaml-profiler/ Latest edition is: "OIOSAML Web SSO Profile 3.0.3"
[OIOSAMLIdP]	https://digst.dk/it-loesninger/standarder/oiosaml-profiler/ Latest edition is: "OIOSAML Local IdP Profile 1.0.3" See also: https://www.mitid-erhverv.dk/avanceret/lokal-idp/
[BPP]	https://digst.dk/it-loesninger/standarder/oiosaml-profiler/ Latest edition is "OIOSAML Basic Privilege Profile 1.2"
[OIOSAML-Java]	https://www.digitaliser.dk/news/6072243
[OIOSAML-NET]	https://www.digitaliser.dk/news/6072243
[OIOSAML2.1.0]	https://www.digitaliser.dk/resource/5833271
[NLBT]	NemLog-in broker terms and conditions. <TBD>
[NLAdm]	https://migrering.nemlog-in.dk/media/kgeliazh/25-brugermanual-til-nemlog-in-administration-v-3.pdf
[NLIDM]	https://migrering.nemlog-in.dk/mitid-erhverv/avanceret-setup/integration-med-idm/
[NLIB]	Integration with NemLog-in for Brokers. https://broker.nemlog-in.dk/dokumentation-og-integration/ - See OIOSAML3 section.
[PP]	Testportal for setting up test organisations: https://testportal.test-devtest4-nemlog-in.dk/ MitID simulator, used for creating test identities: https://mitidsimulator.test-devtest4-nemlog-in.dk Use swagger UI if a test-organisation with specific CVR/name is required: https://testportal.test-devtest4-nemlog-in.dk/swagger/index.html#/Organization/post_api_organization_boextended MitID Erhverv pre-production, Production leg:

Reference	Description
	https://erhvervsadministration.devtest4-nemlog-in.dk MitID Erhverv pre-production, Inttest leg: https://erhvervsadministration.test-devtest4-nemlog-in.dk Pre-production logviewer (inttest leg only): https://logviewer.test-devtest4-nemlog-in.dk/ Metadata for NemLog-in (Service Provider) https://www.nemlog-in.dk/vejledningertiltestmiljo
[MEUG]	MitID Erhverv user guides: https://www.mitid-erhverv.dk/support/ https://www.mitid-erhverv.dk/support/vejledning/anvendelse/#
[DynLinks]	https://firebase.google.com/docs/dynamic-links
[UniLinks]	https://developer.apple.com/ios/universal-links/

13 Appendix A – Creating a test-organisation with Swagger UI

Use the /api/organization/boextended method for creating a test-user organisation. [PP]

Pass parameters in the request body as described below.

Parameter	Description
adminEmail	Your email address. Will be assigned to the test identity created.
password	Password used for the test identity
enableQualifiedCertificates	Boolean indicating if the test organisation is allowed to issue long term qualified certificates. Not relevant for Local IdP integration. Pass false if in doubt.
organizationType	Use either “Private” or “Public” to designate a private/public organisation, respectively. You can use either value when testing local IdP.
createFbrsGroups	Whether to create default rights groups in MitID Erhverv. Not relevant when testing local IdP. Pass true.
uuid	A random UUID generated by you, that will be assigned to the test organisation.
administratorUuid	A random UUID generated by you, that will be assigned to the administrator identity.
physicalPersonIAL	Assurance level of the organisations NSIS-approved registration process. To test Local IdP, pass “Substantial”
name	The name of the test organisation created.
cvrNumber	CVR number of the test organisation created.
adminCpr	Fictitious CPR number for the test identity created.
adminUsername	Username for the test identity created.
adminMaxRegisteredIAL	The maximum identity assurance level that the test administrator can assign to created users. Use “Substantial”.

14 Appendix B – Metadata

14.1 NemLog-in service provider metadata

The metadata describing the NemLog-in Service Provider endpoints can be retrieved online [PP].

14.2 Local IdP sample metadata

```
<?xml version="1.0" encoding="utf-8"?>
<md:EntityDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="_4f022ebe-5055-491f-b0d9-e7c422c98f3c" entityID="https://your-entity-id">
        <md:IDPSSODescriptor WantAuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
                <md:KeyDescriptor use="signing">
                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                <ds:X509Data>
                                        <ds:X509Certificate>MIIGfD…</ds:X509Certificate>
                                </ds:X509Data>
                        </ds:KeyInfo>
                </md:KeyDescriptor>
                <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://your-site.dk/SingleLogout/ServiceProvider/" ResponseLocation="https://your-
site.dk/SingleLogout/LogoutResponse/"/>
                <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
                <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://your-site.dk/SingleSignOn/"/>
                <saml:Attribute Name="https://data.gov.dk/model/core/specVersion" FriendlyName="SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
                <saml:Attribute Name="https://data.gov.dk/concept/core/nsis/loa"
FriendlyName="NSISLevelOfAssurance" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
                <saml:Attribute Name="https://data.gov.dk/model/core/eid/professional/cvr"
FriendlyName="CVR" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
                <saml:Attribute Name="https://data.gov.dk/model/core/eid/professional/orgName"
FriendlyName="OrganizationName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
                <saml:Attribute Name="https://data.gov.dk/model/core/eid/privilegesIntermediate"
FriendlyName="Privileges" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
        </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

14.3 Test-IdP metadata

Metadata for pre-production (inttest-leg) local IdP 0.

```
<?xml version="1.0" encoding="utf-8"?>
<md:EntityDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="_4f022ebe-5055-491f-b0d9-e7c422c98f3c" entityID="https://testlocalidp0-int.sp-devtest4-nemlog-in.dk">
        <md:IDPSSODescriptor WantAuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
                <md:KeyDescriptor use="signing">
                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                <ds:X509Data>

        <ds:X509Certificate>MIIGojCCBNagAwIBAgIUb9Xuxph9IrfUgc6aacM6dvwvn+QwQQYJKoZIhvcNAQEKMDSgDzANBglghkgB
ZQMEAgEFAKEcMBoGCSqGSIb3DQEBCDANBglghkgBZQMEAgEFAKIDAgEgMGsxLTArBgNVBAMMJERlbiBEYW5za2UgU3RhdCBPQ0VTIHVkc3Rl
ZGVuZGUtQ0EgMTETMBEGA1UECwwKVGVzdCAtIGN0aTEYMBYGA1UECgwPRGVuIERhbnNrZSBTdGF0MQswCQYDVQQGEwJESzAeFw0yMzA2MTYw
NzI1NDFaFw0yNjA2MTUwNzI1NDBaMIG4MTQwMgYDVQQDDCtOZW1Mb2ctaW4gVGVzdC5Mb2NhbElkZW50aXR5UHJvdmlkZXIgLSBUZXN0MTcw
NQYDVQQFEy5VSTpESy1POkc6YjRhODc2YzctZDVmMS00NGIzLTlhNmYtNTVjZTU0ZmIzMzg2MSEwHwYDVQQKDBhEaWdpdGFsaXNlcmluZ3Nz
dHlyZWxzZW4xFzAVBgNVBGEMDk5UUkRLLTM0MDUxMTc4MQswCQYDVQQGEwJESzCCAaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGBAOUD
320/1vcScPujAB2hjDU5hDIgLEeeaK8LliazUQpEkDpjcaLAJXNcC8Fzcu/QXAuPO1tYo8E1sTfCiboSeZVgmXlV1nmaUC46TOrNpKovadvw
AuZuQ5E5bRublYkZ39ANhlq+B8tI3XtcdjZldCabKIIXYSCgV5e3grCKoOShC1Q5lcIn7uo6BytT8oM6ZrIhF/IWLVcCPBqV6m4ZOZh91ziY
v+BenqY7pRpD7mcU0sOFTjSMhKmMs1895gpw3Onm3btkJU3Q29KQ0LmT3FHnzbkCKw1TBseRo8Y/D9LRNnDJo2z3mTz5BlOPsulX4hU1BjCQ
JeqMvyFANGqUyne3zMPp842l1KL0yPxbHiATYuiMikux7GoTVmopEdNSWNoFHEGjfkD2e3V/EA4gR3DSEfvO13+/gWNTEAotXy3uM+7NpWFI
WIIvvLnrkT9Ba9Huzpr3CnmjIrAhT3q24R8gc8iopjwgXlSmO86SQLRcAyZY2yKG/p0bG6/5fsaP9wIDAQABo4IBhjCCAYIwDAYDVR0TAQH/
BAIwADAfBgNVHSMEGDAWgBR/KJ/ZcZlC4nXn1zV2Lk0IJW12XjB7BggrBgEFBQcBAQRvMG0wQwYIKwYBBQUHMAKGN2h0dHA6Ly9jYTEuY3Rp
```

```
LWdvdi5kay9vY2VzL2lzc3VpbmcvMS9jYWNlcnQvaXNzdWluZy5jZXIwJgYIKwYBBQUHMAGGGmh0dHA6Ly9jYTEuY3RpLWdvdi5kay9vY3Nw
MCEGA1UdIAQaMBgwCAYGBACPegEBMAwGCiqBUIEpAQEBAwcwOwYIKwYBBQUHAQMELzAtMCsGCCsGAQUFBwsCMB8GBwQAi+xJAQIwFIYSaHR0
cHM6Ly91aWQuZ292LmRrMEUGA1UdHwQ+MDwwOqA4oDaGNGh0dHA6Ly9jYTEuY3RpLWdvdi5kay9vY2VzL2lzc3VpbmcvMS9jcmwvaXNzdWlu
Zy5jcmwwHQYDVR0OBBYEFGnJetiT1t1pS+CYHHsSQ9sKHgk7MA4GA1UdDwEB/wQEAwIFoDBBBgkqhkiG9w0BAQowNKAPMA0GCWCGSAFlAwQC
AQUAoRwwGgYJKoZIhvcNAQEIMA0GCWCGSAFlAwQCAQUAogMCASADggGBAAUGg6S+uFm6qpUY2yLUE+VIaKZizvFoHdwcnFtpUEr3hPR2pSAj
y5jv4wItkC8Vly6wQH+oYjz1uPy4adAQsmHxfdOWjKwq0Uj0oWDuPVpXz0WePN4WmGDoHZka/ULdg7Gy9mikOnafpP4sxStMB+FYtXIj6Wj2
FeUlV3eH4H0CDph41yyxuvmg9PiKSH7R19H7oXx4nPxd8NcJpdYcunSOJdSz5WIwC66EHW8eQQ9NonlS6yC9ky05ygbJQUG4rk1th5G+W9F9
BdMLcNlUMK29mYbzxWncVdlCg6FvbTuQwVTkEGO2U54n8W/2xmdp1KBFSxdR5xLIxk5GYccVO0P65omFwTJ/ZD0vmmN15Q+p5M2qGW1pS5HS
FonjjzuSOOd/I7Sh+ReYOQYCJwcZBc8qvzVdvyU4bfzXtontXAnxpyyNnTiZn4SR+dxYlHphtq/o3tL+wsOurpF3PFoOYDcJ4jS2oC/JbrpB
ok7Rha0gVHqRrmHlY3Ycp6R3z7M6Cg==</ds:X509Certificate>
                                </ds:X509Data>
                        </ds:KeyInfo>
                </md:KeyDescriptor>
                <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://testlocalidp0-int.sp-devtest4-nemlog-in.dk/SingleLogout/ServiceProvider/"
ResponseLocation="https://testlocalidp0-int.sp-devtest4-nemlog-in.dk/SingleLogout/LogoutResponse/"/>
                <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
                <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://testlocalidp0-int.sp-devtest4-nemlog-in.dk/SingleSignOn/"/>
                <saml:Attribute Name="https://data.gov.dk/model/core/specVersion" FriendlyName="SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
                <saml:Attribute Name="https://data.gov.dk/concept/core/nsis/loa"
FriendlyName="NSISLevelOfAssurance" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
                <saml:Attribute Name="https://data.gov.dk/model/core/eid/professional/cvr"
FriendlyName="CVR" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
                <saml:Attribute Name="https://data.gov.dk/model/core/eid/professional/orgName"
FriendlyName="OrganizationName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
                <saml:Attribute Name="https://data.gov.dk/model/core/eid/privilegesIntermediate"
FriendlyName="Privileges" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
        </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Metadata for pre-production (inttest-leg) local IdP 1.

```
<?xml version="1.0" encoding="utf-8"?>
<md:EntityDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="_4f022ebe-5055-491f-b0d9-e7c422c98f3c" entityID="https://testlocalidp1-int.sp-devtest4-nemlog-in.dk">
        <md:IDPSSODescriptor WantAuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
                <md:KeyDescriptor use="signing">
                        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                <ds:X509Data>

        <ds:X509Certificate>MIIGojCCBNagAwIBAgIUb9Xuxph9IrfUgc6aacM6dvwvn+QwQQYJKoZIhvcNAQEKMDSgDzANBglghkgB
ZQMEAgEFAKEcMBoGCSqGSIb3DQEBCDANBglghkgBZQMEAgEFAKIDAgEgMGsxLTArBgNVBAMMJERlbiBEYW5za2UgU3RhdCBPQ0VTIHVkc3Rl
ZGVuZGUtQ0EgMTETMBEGA1UECwwKVGVzdCAtIGN0aTEYMBYGA1UECgwPRGVuIERhbnNrZSBTdGF0MQswCQYDVQQGEwJESzAeFw0yMzA2MTYw
NzI1NDFaFw0yNjA2MTUwNzI1NDBaMIG4MTQwMgYDVQQDDCtOZW1Mb2ctaW4gVGVzdC5Mb2NhbElkZW50aXR5UHJvdmlkZXIgLSBUZXN0MTcw
NQYDVQQFEy5VSTpESy1POkc6YjRhODc2YzctZDVmMS00NGIzLTlhNmYtNTVjZTU0ZmIzMzg2MSEwHwYDVQQKDBhEaWdpdGFsaXNlcmluZ3Nz
dHlyZWxzZW4xFzAVBgNVBGEMDk5UUkRLLTM0MDUxMTc4MQswCQYDVQQGEwJESzCCAaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGBAOUD
320/1vcScPujAB2hjDU5hDIgLEeeaK8LliazUQpEkDpjcaLAJXNcC8Fzcu/QXAuPO1tYo8E1sTfCiboSeZVgmXlV1nmaUC46TOrNpKovadvw
AuZuQ5E5bRublYkZ39ANhlq+B8tI3XtcdjZldCabKIIXYSCgV5e3grCKoOShC1Q5lcIn7uo6BytT8oM6ZrIhF/IWLVcCPBqV6m4ZOZh91ziY
v+BenqY7pRpD7mcU0sOFTjSMhKmMs1895gpw3Onm3btkJU3Q29KQ0LmT3FHnzbkCKw1TBseRo8Y/D9LRNnDJo2z3mTz5BlOPsulX4hU1BjCQ
JeqMvyFANGqUyne3zMPp842l1KL0yPxbHiATYuiMikux7GoTVmopEdNSWNoFHEGjfkD2e3V/EA4gR3DSEfvO13+/gWNTEAotXy3uM+7NpWFI
WIIvvLnrkT9Ba9Huzpr3CnmjIrAhT3q24R8gc8iopjwgXlSmO86SQLRcAyZY2yKG/p0bG6/5fsaP9wIDAQABo4IBhjCCAYIwDAYDVR0TAQH/
BAIwADAfBgNVHSMEGDAWgBR/KJ/ZcZlC4nXn1zV2Lk0IJW12XjB7BggrBgEFBQcBAQRvMG0wQwYIKwYBBQUHMAKGN2h0dHA6Ly9jYTEuY3Rp
LWdvdi5kay9vY2VzL2lzc3VpbmcvMS9jYWNlcnQvaXNzdWluZy5jZXIwJgYIKwYBBQUHMAGGGmh0dHA6Ly9jYTEuY3RpLWdvdi5kay9vY3Nw
MCEGA1UdIAQaMBgwCAYGBACPegEBMAwGCiqBUIEpAQEBAwcwOwYIKwYBBQUHAQMELzAtMCsGCCsGAQUFBwsCMB8GBwQAi+xJAQIwFIYSaHR0
cHM6Ly91aWQuZ292LmRrMEUGA1UdHwQ+MDwwOqA4oDaGNGh0dHA6Ly9jYTEuY3RpLWdvdi5kay9vY2VzL2lzc3VpbmcvMS9jcmwvaXNzdWlu
Zy5jcmwwHQYDVR0OBBYEFGnJetiT1t1pS+CYHHsSQ9sKHgk7MA4GA1UdDwEB/wQEAwIFoDBBBgkqhkiG9w0BAQowNKAPMA0GCWCGSAFlAwQC
AQUAoRwwGgYJKoZIhvcNAQEIMA0GCWCGSAFlAwQCAQUAogMCASADggGBAAUGg6S+uFm6qpUY2yLUE+VIaKZizvFoHdwcnFtpUEr3hPR2pSAj
y5jv4wItkC8Vly6wQH+oYjz1uPy4adAQsmHxfdOWjKwq0Uj0oWDuPVpXz0WePN4WmGDoHZka/ULdg7Gy9mikOnafpP4sxStMB+FYtXIj6Wj2
FeUlV3eH4H0CDph41yyxuvmg9PiKSH7R19H7oXx4nPxd8NcJpdYcunSOJdSz5WIwC66EHW8eQQ9NonlS6yC9ky05ygbJQUG4rk1th5G+W9F9
BdMLcNlUMK29mYbzxWncVdlCg6FvbTuQwVTkEGO2U54n8W/2xmdp1KBFSxdR5xLIxk5GYccVO0P65omFwTJ/ZD0vmmN15Q+p5M2qGW1pS5HS
FonjjzuSOOd/I7Sh+ReYOQYCJwcZBc8qvzVdvyU4bfzXtontXAnxpyyNnTiZn4SR+dxYlHphtq/o3tL+wsOurpF3PFoOYDcJ4jS2oC/JbrpB
ok7Rha0gVHqRrmHlY3Ycp6R3z7M6Cg==</ds:X509Certificate>
                                </ds:X509Data>
                        </ds:KeyInfo>
                </md:KeyDescriptor>
```

```
                <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://testlocalidp1-int.sp-devtest4-nemlog-in.dk/SingleLogout/ServiceProvider/"
ResponseLocation="https://testlocalidp1-int.sp-devtest4-nemlog-in.dk/SingleLogout/LogoutResponse/"/>
                <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
                <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://testlocalidp1-int.sp-devtest4-nemlog-in.dk/SingleSignOn/"/>
                <saml:Attribute Name="https://data.gov.dk/model/core/specVersion" FriendlyName="SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
                <saml:Attribute Name="https://data.gov.dk/concept/core/nsis/loa"
FriendlyName="NSISLevelOfAssurance" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
                <saml:Attribute Name="https://data.gov.dk/model/core/eid/professional/cvr"
FriendlyName="CVR" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
                <saml:Attribute Name="https://data.gov.dk/model/core/eid/professional/orgName"
FriendlyName="OrganizationName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
                <saml:Attribute Name="https://data.gov.dk/model/core/eid/privilegesIntermediate"
FriendlyName="Privileges" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
        </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

15 Appendix C – Assertion

```
<Assertion ID="_5ae7609a-2330-4a7b-8c49-d1da3e16de4f" IssueInstant="2022-10-19T07:44:08.724Z" Version="2.0"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
        <Issuer>https://hammerup.sp-devtest4-nemlog-in.dk</Issuer>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                <SignedInfo>
                        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
                        <Reference URI="#_5ae7609a-2330-4a7b-8c49-d1da3e16de4f">
                                <Transforms>
                                        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                                        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                </Transforms>
                                <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                                <DigestValue>AB8LzF+mqQfwxDqUlaDjQ+rzV/SdM/LsvlscQY27aKA=</DigestValue>
                        </Reference>
                </SignedInfo>

        <SignatureValue>gDRk8Sys9b9EBgIjJ6gkRhUTi72sytYlQghpgmKEPVjjrC4y/l5YDPQswmxXjikTd4iH9blMb3Izz/mapefH
v5+AH1xuriCOOjiRn+ZMCNLxX824eSe9+OLStRHRFFhaBnLQkGNi09wrEhiO1d/CCbhBCzM6uEb83Pzq5GhUCJHZ8NdMAb8V2udmJmaBWmz7
M08E6KSVZ1leg/tEIsAMjMBUCeuuEaJwpLEKiA/e88UUpth2sOCVlvBQ58SLdbJ+qTY6k5qcdtaqUkdFETP1wgJBET+KSoXEg5T5KvIXaX1x
xi9yhMS/4tTyKBm7PyO/WqV1kZh4uVqTZprxqMmvOVmCra0oXTvPNigwF22nIFGul9MAtTDQ8ZeUKfiGTLbR6QLiNov0X8y+3YaYb8S7XP52
iU5xzg+q4xSsbj5R6v8TcdYS2ndqBpveBopKCpM4ZK7d+qgOEsbXE16aYQcE/gwsVaGz3FS7O/X1wSp77zGQrxG7WqFVKTeG7rpmqd4D</Si
gnatureValue>
                <KeyInfo>
                        <X509Data>

        <X509Certificate>MIIGfDCCBLCgAwIBAgIUZ1YmSH0cVIarpR0Gn3rdlpqJjSgwQQYJKoZIhvcNAQEKMDSgDzANBglghkgBZQM
EAgEFAKEcMBoGCSqGSIb3DQEBCDANBglghkgBZQMEAgEFAKIDAgEgMGsxLTArBgNVBAMMJERlbiBEYW5za2UgU3RhdCBPQ0VTIHVkc3RlZGV
uZGUtQ0EgMTETMBEGA1UECwwKVGVzdCAtIGN0aTEYMBYGA1UECgwPRGVuIERhbnNrZSBTdGF0MQswCQYDVQQGEwJESzAeFw0yMjAzMTEwODA
3MDVaFw0yNTAzMTAwODA3MDRaMIGSMRkwFwYDVQQDDBBUZXN0TG9jYWxJZFAgY3RpMTcwNQYDVQQFEy5VSTpESy1POkc6ZWM1ZDBmNzMtMWE
4Zi00YjlhLTg1MmQtZDVkYzVmYmE3YzA3MRYwFAYDVQQKDA1NYWNoaW5lIFRyYWRlMRcwFQYDVQRhDA5OVFJESy04MDEyMzU2NTELMAkGA1U
EBhMCREswggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQDPPoO4h+Ah96XB9dOe3nYR15g+eahPZMA1UvGnXylzFBB5Pw6hTd59IcC
VVphSZ8sVVdfvAeU1NYy2eZJahDNCaVkatO+klmocbhHLxa+Hg5Twm9x/0IsenzmIMvpQ4p39J2Cc1bJrGg7mJTTG82cj6XphR/Mh+0qM0pN
3iL0cCa24pk7nw/Zak0tWAJfWoIHjp8MAVsfRjV8VoLgQif9FW2oB1Hud0ITNpqKwL/1kd5VDVrvHk2UUlPZz9oExM+ZdYBC2U5FbesTCBKa
aQk/1hx6qsJgFzivJZDy/eACh2IRel93Oehh+uwdVFAlCrf1uVMircXYMlxJX00szdKjHdLnaUteiVfnFCIXRryil6R6Wpr0ZKtH/nr+QnS9
dbGlOL9YrphgXHw3hSKwyW1kmcvMlsdDT886NQnRwD6t6U5CurOQ1zU1W3FxQgn7Ah5OuyXmf967MfG75WlhBoMYp6Dr3APVZwxsQh9MAshW
+8mdeVqE4lgZLrQj3Xqku8JMCAwEAAaOCAYYwggGCMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgwFoAUfyif2XGZQuJ159c1di5NCCVtdl4wewY
IKwYBBQUHAQEEbzBtMEMGCCsGAQUFBzAChjdodHRwOi8vY2ExLmN0aS1nb3YuZGsvb2Nlcy9pc3N1aW5nLzEvY2FjZXJ0L2lzc3VpbmcuY2V
yMCYGCCsGAQUFBzABhhpodHRwOi8vY2ExLmN0aS1nb3YuZGsvb2NzcDAhBgNVHSAEGjAYMAgGBgQAj3oBATAMBgoqgVCBKQEBAQMHMDsGCCs
GAQUFBwEDBC8wLTArBggrBgEFBQcLAjAfBgcEAIvsSQECMBSGEmh0dHBzOi8vdWlkLmdvdi5kazBFBgNVHR8EPjA8MDqgOKA2hjRodHRwOi8
vY2ExLmN0aS1nb3YuZGsvb2Nlcy9pc3N1aW5nLzEvY3JsL2lzc3VpbmcuY3JsMB0GA1UdDgQWBBT2cIh3YvZDxCG3Krkk0tQzVKMEmjAOBgN
VHQ8BAf8EBAMCBaAwQQYJKoZIhvcNAQEKMDSgDzANBglghkgBZQMEAgEFAKEcMBoGCSqGSIb3DQEBCDANBglghkgBZQMEAgEFAKIDAgEgA4I
BgQCskwIzEITcfoeimXRQ5Af0kTihkV3uFPZgWWhPrt0mEcI+6fXZbtFz1GsLPvtFUg4p2cCxys62BMkIytLBGWIYuuX4z1zsw1UF0HKT6y+
sQWrVzLXmOZpYNpV+Vfit7EvagYNAUc8F3SpzQLVUdzHcqorMbmOhpQYjPbg3Z70j6onSZkg128kMGXO4if0//wCN35obViBHfb5O+MReVnh
cMYIcSB+fj/D8W+ldSw9GFV8QpbjJqAD6bzjTRKweg/wjGv+rByr6UTA2v3UjRJHxkFi0fXknkynSunedTw5r1j2JymIMjzRul2iV+/Bo0FU
vTaw0gNNCgVzgA50GR/wZk4SZlBasTt4omPStqshW+yM5l/af32PmvNi5NKM9GA8zUZJgac+nv5KXdRQHYY5DC/QnEslDVcd7mQ6RV2SlV+o
oe30IhMog4KXDb73nAjdY0l7+rcQ2gOcEQ3khVPgv6tL4fEH/xE5RKoXUAGh1CpNY8k6SZdQFMdTTtp7p8pE=</X509Certificate>
                        </X509Data>
                </KeyInfo>
        </Signature>
        <Subject>
                <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">thomasnymand</NameID>
                <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                        <SubjectConfirmationData InResponseTo="_7a018ef1-f4be-a6bc-089e-ed23ccdf7d7f"
NotOnOrAfter="2022-10-19T07:54:08.724Z" Recipient="https://test-devtest4-nemlog-in.dk/localidp/saml/1.0/"/>
                </SubjectConfirmation>
        </Subject>
        <Conditions NotBefore="2022-10-19T07:44:08.708Z" NotOnOrAfter="2022-10-19T07:54:08.708Z">
                <AudienceRestriction>
                        <Audience>https://saml.test-devtest4-nemlog-in.dk</Audience>
                </AudienceRestriction>
        </Conditions>
        <AttributeStatement>
                <Attribute Name="https://data.gov.dk/model/core/specVersion"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                        <AttributeValue>OIO-SAML-3.0</AttributeValue>
```

```
                </Attribute>
                <Attribute Name="https://data.gov.dk/model/core/eid/professional/cvr"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                        <AttributeValue>91636003</AttributeValue>
                </Attribute>
                <Attribute Name="https://data.gov.dk/concept/core/nsis/loa"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
                        <AttributeValue>Substantial</AttributeValue>
                </Attribute>
                <Attribute Name="https://data.gov.dk/model/core/eid/privilegesIntermediate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

        <AttributeValue>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4NCjxicHA6UHJpdmlsZWdlTGlzdCB4bWxu
czpicHA9Imh0dHA6Ly9kaWdzdC5kay9vaW9zYW1sL2Jhc2ljX3ByaXZpbGVnZV9wcm9maWxlIiB4bWxuczp4c2k9Imh0dHA6Ly93d3cudzMu
b3JnLzIwMDEvWE1MU2NoZW1hLWluc3RhbmNlIiA+DQogICAgPFByaXZpbGVnZUdyb3VwIFNjb3BlPSJ1cm46ZGs6Z292ZW9nNhbWw6Y3ZyTnVt
YmVySWRlbnRpZmllcjo5MTYzNjAwMyI+DQogICAgICAgICAgICAgICAgPC9QcmlsZWdlR2VHcm91cD4NCjwvYnBwOlByaXZpbGVnZUxpc3Q+</AttributeValue>
                </Attribute>
        </AttributeStatement>
        <AuthnStatement AuthnInstant="2022-10-19T07:44:08.708Z" SessionIndex="24-28-6E-DC-94-31-95-0E-49-72-
70-57-F8-05-53-8A-25-60-6A-42">
                <AuthnContext>
                        <AuthnContextClassRef>https://data.gov.dk/concept/core/nsis</AuthnContextClassRef>
                </AuthnContext>
        </AuthnStatement>
</Assertion>
```

16 Appendix D – XML schema for public SAML extensions

```
<?xml version="1.0" encoding="UTF-8" ?>
<schema
        targetNamespace="https://data.gov.dk/eid/saml/extensions"
        xmlns:publicExtensions="https://data.gov.dk/eid/saml/extensions"
        xmlns="http://www.w3.org/2001/XMLSchema"
        elementFormDefault="qualified"
        blockDefault="substitution"
        version="2.0">
    <element name="Platform" type="publicExtensions:AppSwitchPlatformType" />
    <simpleType name="AppSwitchPlatformType">
        <restriction base="string">
            <enumeration value="Android" />
            <enumeration value="iOS" />
        </restriction>
    </simpleType>
    <element name="ReturnURL" type="anyURI" />
    <element name="AppSwitch" type="publicExtensions:AppSwitchType" />
    <complexType name="AppSwitchType">
        <sequence>
            <element ref="publicExtensions:Platform" />
            <element ref="publicExtensions:ReturnURL" />
        </sequence>
    </complexType>
</schema>
```