DIGITALISERINGSSTYRELSEN

NemLog-in

# Integration with NemLog-in for brokers

# Contents

# Changelog

| Date | Version | Change description |
|---|---|---|
| 22-01-2021 | 0.1 | Initial version |
| 07-02-2021 | 0.2 | Added feedback from DIGST |
| 15-04-2021 | 0.3 | Removed handled comments.<br><br>Updated links to ref. implementations. |
| 06-09-2022 | 0.4 | Updated layout and minor typos |
| 12-12-2023 | 0.5 | Updated requirement in section 4.5 of calling the GetAttributes endpoint in the Identity Service, when using the advanced scenario of authenticating an employee. Updated to reflect the availability of local IdPs as a possible upstream IdP. |
| 11-01-2024 | 0.6 | Specified the use of ProviderName in the Authentication Request |
| 02-05-2024 | 0.7 | Removed all references to NemID OCES2 |
| 07-05-2024 | 0.8 | Adjusted section 6.1.1 regarding allowed special characters in ProviderName |

Update the footer w. date and version as well.

# 1 Introduction

This document describes how authentication brokers should be integrated with the NemLog-in3 OIO SAML interfaces.

An (authentication) broker acts as an intermediary between its associated service providers (usually considered clients or customers to the broker) and identification providers/identification services. The broker thus allows service providers to use a (broad) set of means of identification unified in a single integration. As such the broker decouples the service provider from the complexity of handling multiple authentication methods.

NemLog-in already supports brokers, previously referred to as Gateway suppliers ("Gateway leverandører)". In the new NemLog-in the broker scope is broadened since the brokers are allowed access to more interfaces, allowing the broker to devise a more elegant user experience to customers. The new options are accompanied by a corresponding set of obligations, most prominently the obligation to become NSIS compliant.

Brokers integrate with NemLog-in3 by a set of interfaces, most notably the OIO SAML 3.0.3 interface. In that sense the broker acts as a service provider, but with an extended set of options and responsibilities. First of all, a broker must be NSIS compliant, and a broker system will not be connected to NemLog-in (production) until that has been verified and reported to the Danish Agency for Digitisation (DIGST).

Brokers whose service providers need access to NemLog-in employee identities (administered by the user organisations in the MitID Erhverv application) must be connected to NemLog-in as a broker system.

## 1.1 Prerequisites

This document should be read as an extension to [NLI] which should be read before this document.

The reader is expected to be familiar with the most recent version of the OIO SAML 3 profile [OIOSAML3].

The NemLog-in broker terms and conditions [NLBT] describe important requirements that the broker must adhere to.

## 1.2 Intended audience

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

## 1.3 Terminology

| Term | Description |
|---|---|
| Identity Provider | 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. |

| Term | Description |
|---|---|
| Broker | A Broker serves as an intermediary between the SP and the IdP, see section 4 below. |
| 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, 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:<br>• Entity ID – a unique identifier for the party (SP/IdP) in the federation<br>• Cryptographic keys in the form of X.509 certificates - used for signing and encryption.<br>• Protocol endpoints |
| Local IdP | In NemLog-in3 the 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 a NSIS compliance by the user organisation. |

# 2 Reference implementations

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

For this reason, we strongly recommend that your integration with NemLog-in makes use of available SAML software, preferably one of the available OIO SAML reference implementations:

- OIO SAML for Java – [OIOSAML-Java]
- OIO SAML for C#/.NET – [OIOSAML-NET]

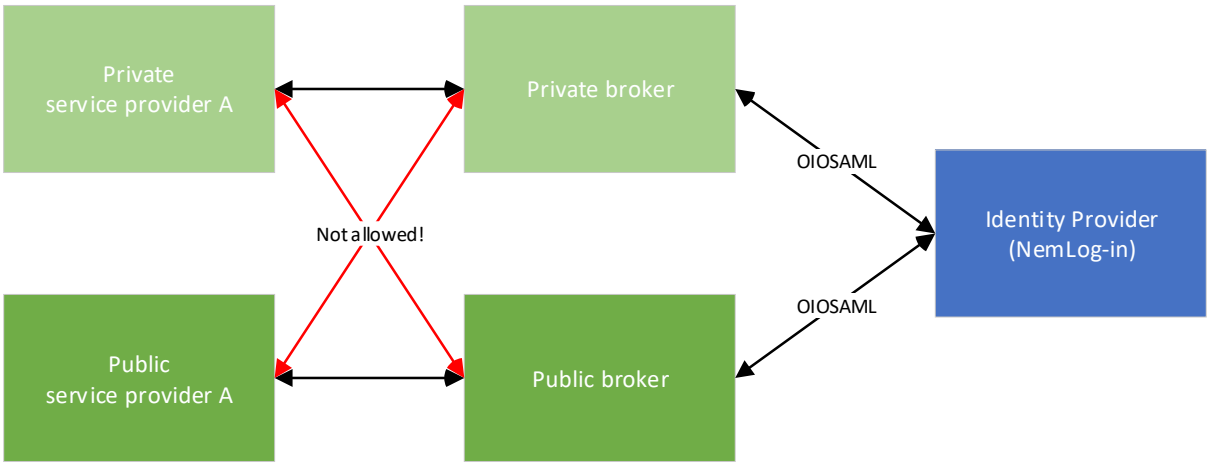
These software packages provide sample code and demonstration applications for both authentication and attribute query integrations.

Even if you plan use another SAML implementation the reference implementations will be very useful to allow developers to familiarize themselves with the SAML protocol and OIO SAML specifics.

# 3 Public and private brokers

NemLog-in3 functionality is available to both public and private brokers. A public broker is a broker that acts as an authentication proxy for public service providers, a private broker acts as an authentication proxy for private service providers. Note, that a public *organisation* may connect a *private* broker, and vice versa.

Further note, that the nature of a given broker limits the types of service providers that may be connected: An organisation that wishes to provide broker services to both private and public service providers are obliged to connect two broker systems, one for each type of service provider, as illustrated by the figure below.




**Figur 1: Public and private brokers**

Some NemLog-in features are only available to public brokers, these are summarised in the table below.

| Feature | Available to public brokers | Available to private brokers | Remarks |
|---|---|---|---|
| OIO SAML 2.1.0 interface | No[1] | No | Neither public or private brokers are allowed to use the deprecated OIO SAML 2 protocol |
| OIO SAML 3.0.3 interface | Yes | Yes | |
| Attribute Service | Yes | Yes | The NemLog-in Attribute Service could be used to enhance end-user privacy by allowing the broker to only request a minimal attribute set during authentication and then subsequently request additional attributes. |

[1] Access could be obtained by connecting the system as “Gateway supplier” but is not recommended.

| Feature | Available to public brokers | Available to private brokers | Remarks |
|---|---|---|---|
| Single Sign-on | Yes | No | Public brokers using the simple integration model will participate in NemLog-in SSO. Note, that although private brokers are not participating in SSO they must nevertheless implement the Single log-out profile. |
| Single Logout (SLO) | Yes (required) | Yes (required) | Even though private brokers are not allowed participation in NemLog-in SSO they must implement support for SLO. |
| FBRS access rights | Yes | No | Private brokers are not allowed to specify the Privileges attribute in metadata. See [OIOSAML3], section 6.2.3. |
| CPR attribute | Yes | No | Private brokers are not allowed to specify the CPR attribute in metadata. This also prevents access to CPR attributes by Attribute Query. We refer to [NLI] for details on how private brokers should obtain CPR numbers (use of NemLog-in PID-CPR-match). |

# 4 Architectural overview

With the MitID Erhverv identities it is relevant for brokers to select an integration model. NemLog-in supports two different integration models, *simple* integration, and *advanced* integration.

In the simple integration model the broker uses a minimum of the available interfaces. This lowers the implementation cost and complexity but the end users accessing service providers connected to the broker will interact directly with NemLog-in user interface.

In the advanced integration model the broker uses an extended set of interfaces. By using the model, the service providers connected to the broker will only interact with the user interface provided by the broker. This will allow the broker to completely control the user experience for the end-users.

## 4.1 Simple integration

In the simple model, the broker acts as a SAML proxy for the connected service providers as depicted in the figure below.

**Figure 1: Simple broker integration model**

NemLog-in controls the integration to MitID. This means that the MitID user interface will not show the friendly name of the requesting service provider but that of the broker. E.g., “Log in at <broker friendly name>”, not “Log in at <service provider friendly name>”.

With the availability of local IdPs to user organisations the change is transparent to the brokers; the broker (or service provider) is generally not able to distinguish the applied identifications means in a particular authentication flow in the simple integration model.

## 4.2 Advanced integration with MitID

In the advanced integration model, the broker integrates directly to MitID. When (and if) the service provider requests an employee identity, the broker queries NemLog-in using the Identity Service API for MitID Erhverv employee identities associated to the used private identification. The available employee identities are displayed in the broker UI and the end-users selects an identity. The broker then requests a set of attributes for the selected employee identity.

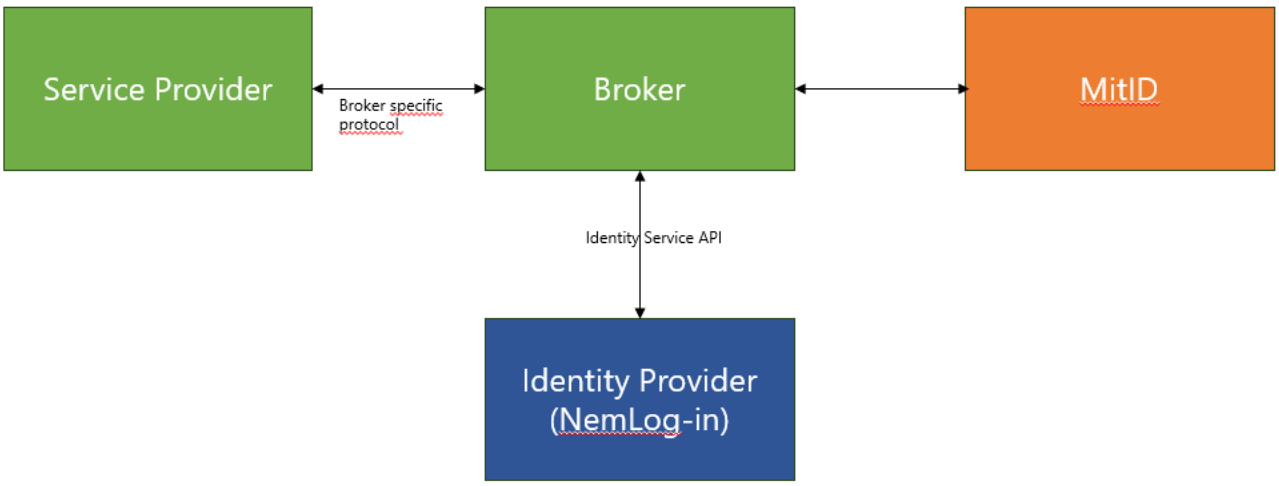



**Figure 2: Advanced broker integration**

Note that NemLog-in is only involved for authentications involving MitID Erhverv identities. If only private identities are required by the brokers service providers, no NemLog-in integration is required.

## 4.3 Advanced integration, local IdP

The advanced integration model supports local IdPs in such a way that the users do not interact with the NemLog-in user interface.

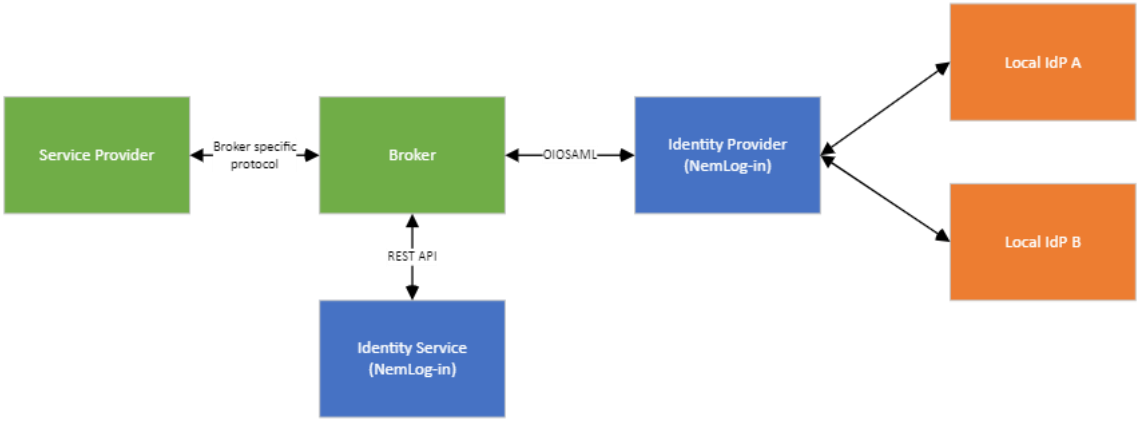



**Figure 3: Advanced integration with local IdP**

This requires a more advanced integration to NemLog-in involving both API access (Identity Service API) to retrieve information about connected local IdPs, see section 4.6 of [NLIDM], and advanced SAML integration where the broker specifies the upstream local IdP to be used to bypass user interaction with NemLog-in, see section 9.8 of [NLI].

## 4.4 Interaction scenarios, simple

In the simple integration model, the broker acts as a service provides with respect to NemLog-in. For interaction scenarios we therefore refer to [NLI].

## 4.5 Employee authentication with MitID, advanced

This scenario shows how a user can perform an authentication using a MitID identification means for a MitID Erhverv employee identity in the advanced broker integration setup.

In this scenario the broker only accesses NemLog-in by API (Identity Service).

Note, that the broker chooses the authentication protocol to use for his own service providers. In this scenario a SAML-like protocol involving browser redirects is suggested but this is entirely at the brokers discretion.

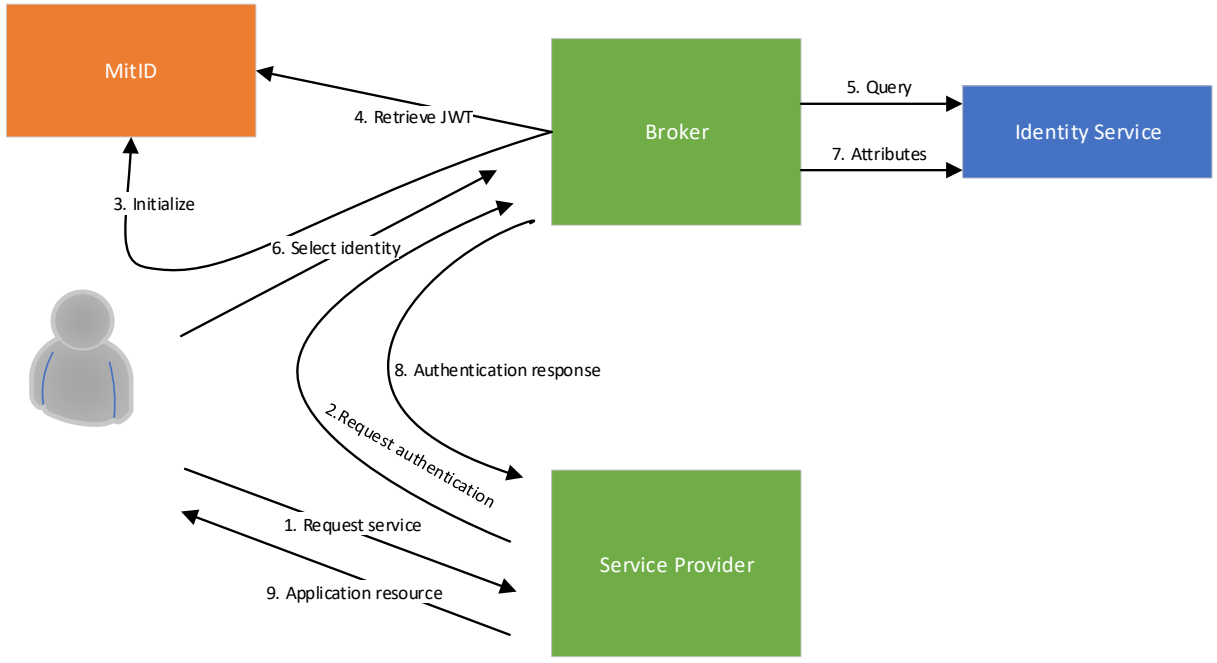



**Figure 4: Employee authentication with MitID in the advanced integration model**

The steps are:

1. The user requests a service at the brokers SP.
2. The service provider has no session with the user and requests authentication using the brokers authentication protocol.
3. The broker initialises the MitID authentication client that he uses, and the user interacts with the MitID client to authenticate. In the process the user uses the appropriate identification means for the required assurance level.
4. The broker learns that the MitID authentication has finalised and requests the MitID authentication response (JWT) using the MitID protocol.

5. The broker knows that the service provider accepts an employee log in and therefore queries the NemLog-in Identity Service to learn if any employee identities are associated to the particular MitID eID.
6. The broker presents the available employee identities to the user. The user selects one of these identities.
7. The broker requests the attributes for the selected identity by invoking the Identity Service once more. This call is mandatory even if the broker does not require extra attributes to produce the authentication response. In this case simply supply an empty collection of optional attributes.
8. The broker produces an authentication response and returns the user to the service provider.
9. The service provider validates the broker authentication response, creates a user session, and returns the requested resource to the user.

In this scenario the broker must consider if a user consent is required before sensitive attributes are released to the service provider. A consent interaction would take place between steps 7 and 8.

# 5 NemLog-in interfaces for brokers

NemLog-in provides a set of interfaces available to service providers. Those interfaces are also available to brokers and are described in [NLI].

In addition to these, NemLog-in provides a set of interfaces that are exclusive for brokers. These are described in the table below.

| Interface/API | Description |
|---|---|
| Identity Service | The Identity Service API allows brokers to provide MitID Erhverv identities to service providers. The API has methods for requesting employee identities associated to a particular MitID and for obtaining attributes for employee identities. Brokers can also obtain a list of active Local IdP systems including friendly names and EntityIDs.<br>Access to the Identity Service interface is obtained by choosing Advanced Broker Services when the broker system is connected to NemLog-in in Administration. We refer to the Administration user guide for details [NLAdm].<br>The Identity Service API is documented in [NLIDM], consult this reference for details. |
| Signing API | Brokers can use the qualified signing service in the same way that service providers do. This entails that the end user experience will involve interactions with the NemLog-in UI. If the broker wishes to completely control the signing user experience the broker can develop his own signing client which directly interacts with NemLog-in signing services by API.<br>Note that this approach requires the brokers signing client to be certified according to ETSI standards.<br><br>We refer to [NLBS] for details.<br><br>The broker signing API is selected by choosing “Services for Brokers own Signing Client” when connecting the system in NemLog-in Administration. See [NLAdm] |

# 6 SAML integration

Brokers using the simple integration model use the SAML integration to NemLog-in. In this case brokers act as SAML service providers wrt. NemLog-in and we refer to [NLI] for integration details.

The additional details relevant for broker SAML integrations with NemLog-in are described in this section.

## 6.1 Authentication requests

When requesting authentication, brokers must adhere to the [OIOSAML3] specification and may use of the functionality described in [NLI] that is also available to service providers.

Brokers have additional options and must conform to additional requirements, which are described in this section.

### 6.1.1 Specifying the requesting service provider

Brokers are required to specify the service provider identity as detailed in [OIOSAML3], OIO-SP-09. Please note that to support special characters the ProviderName must be defined as an UTF-8 string Base64 encoded in the attribute. It must consist of between 2 and 100 characters. The following character set is allowed:

- Letters and numbers including ÆØÅ
- Special characters: .,()-\/
- Blank space

This information is forwarded to the local IdP.

# 7 References

Most documentation is available here: https://broker.nemlog-in.dk/forside/.

| Reference | Description |
|---|---|
| [NLI] | 10 Integration with NemLog-in |
| [OIOSAML3] | https://digst.dk/it-loesninger/standarder/oiosaml-profiler/ |
| [OIOSAML-Java] | https://github.com/digst/OIOSAML.Java |
| [OIOSAML-NET] | https://github.com/digst/OIOSAML.Net |
| [OIOSAML2.1.0] | https://digst.dk/it-loesninger/standarder/oiosaml-profiler/ |
| [NLBT] | https://broker.nemlog-in.dk/tekniske-krav-vilkar-og-priser/aftale-og-vilkar/ |
| [NLAdm] | https://tu.nemlog-in.dk/oprettelse-og-administration-af-tjenester/brugermanual-til-nemlog-in-administration/ |
| [NLIDM] | https://broker.nemlog-in.dk/dokumentation.og.integration/ |
| [NLBS] | 17 NL3 Signing - Broker implementation guidelines https://migrering.nemlog-in.dk/media/fcej4wyk/signeringsdokumentation-v1-0-1.zip |