



SignaturGruppen



Version 0.9.1 2022



Table of Contents

Table of Contents	2
Nets eID Broker documentation documents	3
Changelog	4
Version 0.1	4
Version 0.9	4
Introduction	4
MitID Erhverv and NemLog-In EIA	4
MitID Private ID authenticators	4
MitID Erhverv dedicated authenticators	4
NSIS Local IdP	5
User administration in NemLog-In EIA	5
MitID Erhverv integration in Nets eID Broker	5
Returned claims	5
MitID Erhverv test-users	6
Specific configurations	7



Nets eID Broker documentation documents

This document services a source of documentation for the MitID Erhverv solution and gives information of how it can be tested. The collected list of technical documents for NEB is listed here.

All documents can be found at <https://broker.signaturgruppen.dk/>

Title	Description
Nets eID Broker Technical Reference [NEB-TECHREF]	The primary source of technical documentation for the integration to Nets eID Broker (this document).
Nets eID Broker Frontend Guide [NEB-FRONTEND]	Examples and guides for the frontend integration to Nets eID Broker and OpenID Connect in general. Also covering mobile apps.
Nets eID Broker Sessions [NEB-SESSIONS]	Technical information about sessions in the NEB platform. Contains information about how NEB handles session and the various ways service providers can utilize and handle this in their integration.
Nets eID Broker OpenID Connect Intro [NEB-INTRO]	
Nets eID Broker Identity Providers [NEB-IDP]	Contains technical information about the available identity providers supported by NEB.



Changelog

Version 0.1

First version.

Version 0.9

Updates with examples for configurations.

Version 0.9.1

Updates with new user examples. Please note that some of the previous test-users are permanently broken

Introduction

This document describes the various options for MitID Erhverv. Note that the document is only intended to introduce the MitID Erhverv setup as well as how it works in combination with the Nets eID Broker.

The intended audiences are IT developers, architects, and integration testers.

Business functionality specified in this document may be subject to different commercial agreement requirements.

General information, online demonstration, documentation (including the newest version of this document) and example code is found at <https://broker.signaturgruppen.dk>.

Note that for in-depth information on Nemlog-in and the MitID Erhverv solution the reader is referred to <https://digst.dk/it-loesninger/nemlog-in/>.

MitID Erhverv and NemLog-In EIA

As mentioned, it is expected that the reader will have some knowledge of how NemID, MitID and NemLog-In work. This section serves as a summary. Private citizens can use MitID authentication to login with their private identity. Employees in companies can login in different ways with MitID than was the case with the previous NemID authentication setup, where only dedicated NemID OTP/keyfile could be used. The different options are listed below. Regardless of how the user logs in to his MitID Erhverv role the service provider will get access to the same identity information of the employee.

MitID Private ID authenticators

If both the user and the company where the user is employed agree to use this option, it is possible to let the user re-use his private identity and corresponding MitID authenticators to login.

Note also that private MitID or NemID logins can be stepped up through the so-called private-to-business mechanism where companies associated to the users CPR number can be looked up in the Erhvervsstyrelsen company register. This is a different mechanism than MitID Erhverv and will require the user to enter his CPR number. It is expected that these company associations will be a part of the standard MitID Erhverv at some point.

MitID Erhverv dedicated authenticators

The company administrator can assign a dedicated MitID Authenticator to the user. This could be any of the approved MitID authenticators known from the MitID Private solution. This can be

- 1) MitID Authenticator App
- 2) MitID OTP device/codereader
- 3) MitID Chip

The login process is similar to that of ordinary MitID known for private IDs.



NSIS Local IdP

Some large user organizations are expected to implement a so-called identity provider (IdP). Read more on the solution at <https://digst.dk/it-loesninger/nemlog-in/om-loesningen/aendring-i-funktionaliteter/lokal-idp/>. With a local IdP the user organization has the responsibility to verify the user identity and provide the user with authenticators to be able to authenticate the user in a secure manner to obtain the various security levels identified in the NSIS standard framework. With a local IdP the login process is handled between Nemlog-in and the local IdP, however the service provider will after successful authentication receive the usual set of user information.

User administration in NemLog-In EIA

Employees are administered in the EIA-system by company administrators. This process is not described in this document. Note that an employee can be assigned any combination of the above mentioned authentication setups. For testing MitID Erhverv users can log-in to their self-service at <https://erhvervsadministration.test-devtest4-nemlog-in.dk/>

MitID Erhverv integration in Nets eID Broker

For a service provider to be able to use MitID Erhverv identities through the Nets eID Broker a special scope (nemlogin) should be used to get the relevant employee information and further the login process is initiated using a special identity provider through the configuration of idp_value (mitid_erhverv). The login process will then support the above-mentioned ways of logging in, however currently the local Idp option is not available in any of the Nemlog-in systems. Note that MitID Erhverv will need to be set up for a given service provider by the Nets eID Broker administration before it can be used.

When the user is logging in, he will be prompted to select between identities assigned to the used authenticator if more than one is available. Note that if a MitID Private authenticator is used the integration can be setup to allow the user to not complete the anticipated MitID Erhverv login but instead complete the login as the associated private identity.

Returned claims

If the user ends up logging in to his employee identity the following special claims are returned from the user info endpoint:

Claim	Value
nemlogin.date_of_birth	Employee birthday
nemlogin.email	Employee e-mail (may be empty)
nemlogin.name	Employee Name (note for anonymous users)
nemlogin.family_name	Employee Family Name (note for anonymous users)
nemlogin.given_name	Employee First Name (note for anonymous users)
nemlogin.nemid.rid	Employee certificate RID from NemID migration (or assigned)
nemlogin.org_name	Company Name
nemlogin.persistent_professional_id	MitID Erhvervs Global UUID/ID from EIA
nemlogin.cvr	Company CVR
nemlogin.se_number	Company SE number (may be empty)
nemlogin.p_number	Company P number (may be empty)



To be able to recognize the user on sub_sequent logins it is recommended to persist the persistent_professional_id which is the global identifier. However, as with other logins through the Nets eID Broker the sub-claim from the id_token can also be used to recognize the user. Note also that it is also recommended to verify that the expected identity type is returned as a result of the login process.

MitID Erhverv test-users

The Nets eID Broker test/pp-system is wired up to use the so-called NemLog-In test-devtest4 environment. This relies on a couple of sub-systems. However, to test basic functionality it is not important to know anything else than how to use the ordinary MitID PP test-tool. For testing a few test-identities have been set up and details are provided in the tables below. To be able to test migration of existing users NemID Erhverv users a few of the users are equipped with corresponding NemID Erhverv key-files which can be located on the provided links.

User with both MitID Private and dedicated authenticator

CPR: 1109532297

MitID Privat ID: Gustav4190

MitID Erhverv ID: Gustav4erhverv

MitID Erhverv EIA UUID: d797bc7a-b20a-41b3-89c6-f74f2ac2ed2a

NemID Erhverv RID: 64284701 (CVR: 29915938)

(https://www.signaturgruppen.dk/download/mitiderhverv/Gustav_Poulsen2.zip (PW: Test1234))

User with only MitID Private authenticator

CPR: 2110035775

MitID Privat ID: Mathias60249

MitID Erhverv EIA UUID: e0930d2a-7b16-41d4-96ca-e0d38c5d5122 (CVR: 29915938)

NemID Erhverv RID: 59810192 (CVR: 29915938)

(https://www.signaturgruppen.dk/download/mitiderhverv/Mathias_Hansen2.zip (PW: Test1234))

User with only dedicated MitID employee authenticator

CPR: 1206421505

MitID Erhverv ID: Christian9erhverv

MitID Erhverv EIA UUID: 7b728b3e-7e2a-494b-a4fa-4c1d1a6b3ba6 (CVR: 29915938)

NemID Erhverv RID: 32471538 (CVR: 29915938)

(https://www.signaturgruppen.dk/download/mitiderhverv/Christian_Petersen2.zip (PW: Test1234))

User with multiple company identities

CPR: 1005843029

MitID Privat ID: Alf1343

MitID Erhverv EIA UUID: 021bcbe0-6625-4514-a1cd-850ed9077732 (CVR: 29915938)

NemID Erhverv RID: 51627192 (CVR: 29915938)

(https://www.signaturgruppen.dk/download/mitiderhverv/Alf_Poulsen2.zip (PW: Test1234))

MitID Erhverv EIA UUID: bb947b7e-81a7-453e-9823-e78185935651 (CVR: 26382122)

NemID Erhverv RID: 42869515 (CVR: 26382122)



Specific configurations

Below is a list of relevant configurations to consider when planning your employee login solution. For reference a few configurations for NemID Erhverv is also described.

Basic MitID Erhverv configuration

In order to receive only basic MitID Erhverv logged-in users the configuration below can be used. Note that it will only allow users with a valid MitID Erhverv Identity to log in (based on either a private MitID authenticator or a dedicated MitID Erhverv authenticator).

```
idp_values: mitid_erhverv
scope: openid nemlogin
```

MitID Erhverv configuration allowing also private MitID users

Besides the basic MitID Erhverv users private MitID users will also be allowed. Note that the identity information is received in mitid.-claims. Private MitID sessions can be stepped up with the private_to_business-scope.

```
idp_values: mitid_erhverv
scope: openid mitid nemlogin
idp_params: "mitid_erhverv":{"allow_private":true}
```

NemID Erhverv configuration allowing also private NemID users

Besides the basic NemID Erhverv users private NemID users with mappings to companies will also be allowed. Private NemID sessions will be attempted to be stepped up with the private_to_business-scope. Note that a user that logs in with a private NemID identity in order to attempt private_to_business step-up may continue without any such mapping.

```
idp_values: nemid
scope: openid nemid private_to_business
idp_params: "nemid":{"amr_values":"nemid.otp nemid.keyfile"}
```

Basic NemID configuration

Besides the basic NemID Erhverv users private NemID users will also be allowed. For private identities the SSN/CPR-step-up process can be followed.

```
idp_values: nemid
scope: openid nemid ssn
idp_params: "nemid":{"amr_values":"nemid.otp nemid.keyfile"}
```