Agency for Digital Government

TERMS AND CONDITIONS FOR USE OF LOCAL IDP

Annex 7

Version: 1.4

Author: Danish Agency for Digital Government, MitID Erhverv

Publication Date: March 2026

Erhverv

Table of Contents

The terms and conditions are written in Danish and translated into English. The Danish-language version shall be authoritative in all respects and shall prevail in the event of any inconsistency with the English translation.

Erhverv

1.Introduction

These Terms govern a User Organisation's use of a Local IdP with MitID Business via NemLog-in's broker.

Using a local IdP allows a User Organisation to locally manage its own Business Identities and Authenticators, which allows, among other things:

- Business users can use the same local Authenticators in their own organisation as well as towards externally directed Digital Self Service solutions connected to NemLog-in's Broker and other brokers connected to NemLog-in that support authentication with a Local IdP.
- The User Organisation can achieve a simpler administration of Business Users by managing them only locally and synchronising updates with MitID Business via API.

The assignment and configuration of a Local IdP to the User Organisation and adherence to these Terms shall be done by the User Organisation's Organisation Administrator.

These Terms are governed in their entirety by the Terms for User Organisations. In the event of any conflict, the Terms for User Organisations shall prevail.

Not all Services described in these Terms may be available at the time of the User Organisation's acceptance of the Terms. The User Organisation must refer to the MitID Business Portal separately for a detailed description of which Services are available as well as possible schedules for the introduction of new Services.

The Annexes to the Conditions form an integral part thereof.

2.Contact information

The Agency for Digital Government has the following contact information:

The Agency for Digital Government
Attn. MitID-Erhverv
Landgreven 4
1301 Copenhagen K
E-mail: **mitiderhverv@digst.dk**

3.Definitions

Defined terms follow definitions set out in the Terms for User Organisations.

4. NSIS notification and compliance with NSIS

4.1 NSIS Notification or eIDAS conformity assessment and Maintenance Thereof

Prior to the use of a Local IdP in MitID Erhverv, the Local IdP must be registered with NSIS as an electronic identification scheme and identity broker at minimum Identity Assurance Level Substantial. The NSIS notification is only completed when the Local IdP is included on The Agency for Digital Government NSIS positive list.

Alternatively, the Local IdP may be subject to eIDAS conformity assessment by an approved conformity assessment body in accordance with the standard ETSI TS 119 461 with the target LoIP Extended.

The NSIS notification or eIDAS conformity assessment must be maintained on an ongoing basis, cf. clause 9 below.

4.2 Usage Models for Local IdP

A Local IdP can be used according to two models: 1) Local IdP at the User Organisation and 2) Use via Full-service Local IdP with a third party.

Re. Model 1 Local IdP at User Organisation

The User Organisation submits an NSIS notification or obtains an eIDAS conformity assessment of its own Local IdP and is subject to the audit required under NSIS or ETSI TS 119 461, including in relation to technical solutions and processes. The User Organisation may have a subcontractor perform certain subtasks, provided this is stated in the NSIS notification and audit statement or eIDAS conformity assessment report.

Model 1 also covers Local IdPs that are part of a joint NSIS notification or eIDAS conformity assessment from several User Organisations, where all User Organisations are listed in the same notification and audit statement or eIDAS conformity assessment report.

Under Model 1, the User Organisation appears on the NSIS positive list regardless of whether the User Organisation is NSIS notified alone or covered by a joint notification, unless the User Organisation has obtained an eIDAS conformity assessment.

Re. Model 2 Full-service Local IdP

The User Organisation uses a Local IdP provided by a third party. The third party has notified the Local IdP or has been eIDAS conformity assessed and handles all technical and procedural matters regulated in NSIS and ETSI TS 119 461 respectively, including registration and identity assurance of users and issuance of Authenticators for NSIS, in particular, the requirements in clause 3.1.3. The external Full-service Local IdP is subject to the audit required under NSIS or the eIDAS Regulation. Under Model 2, the third party appears in the NSIS Positive List or holds an eIDAS conformity assessment report.

User Organisations that wish to use a Full-service Local IdP according to model 2 is obliged to sign the management declaration listed in Annex A and submit it to MitID Erhverv, cf. clause 2.

The management declaration can also be downloaded from:

https://mitid-erhverv.dk/en/advanced-functionalities-in-mitid-erhverv/local-idp/management-statement-and-joint-management-statement-for-idp/

The User Organisation shall be fully responsible for the Local IdP used and for ensuring that all the requirements set out in the Terms are met, regardless of whether a Local IdP is used under model 1) or model 2).

4.3 Special Restrictions for User Organisations Using a FullService Local IdP

To enable the technical connection of a FullService Local IdP, the User Organisation is granted access equivalent to that granted to an NSIS-notified or eIDAS conformity assessed User Organisation.

A User Organisation that uses a FullService Local IdP in MitID Erhverv, cf. model 2 above, and has neither registered a Local IdP under NSIS nor gotten it eIDAS conformity assessed, may only accept invitations from a Full Service Local IdP and is not permitted to connect its own Local IdP to MitID Erhverv.

User Organisations that are not themselves registered under NSIS or eIDAS conformity assessed are therefore not permitted to immediately create their own identities with an NSIS assurance level or LoIP Extended, nor may they create administrators who can immediately create identities[1]. All activation of the User Organisation's users must therefore take place via an NSIS-registered solution (either MitID Erhverv or an NSIS-registered Local IdP) or an eIDAS conformity assessed solution (either MitID Erhverv or an eIDAS conformity assessed Local IdP)

5.Local IdP and MitID Erhverv

5.1 Creating Business Identities in MitID Erhverv

A prerequisite for a Business User to be authenticated through a Local IdP connected to MitID Erhverv is that the Business User is set up with an association to the User Organisation in MitID Erhverv and that the Business User is registered in MitID Erhverv to be able to use a local Authenticator.

The user organisation can create Identities in MitID Erhverv in the following ways:

- Via the user interface of MitID Erhverv

[1] In the MitID Erhverv user interface, it is the checkbox 'Is educated to create users at substantial assurance level' that must not be selected for the User Organisation's administrators when the User Organisation itself is not notified under NSIS.

- Via IdM API interface exposed by MitID Erhverv

The creation of Business Users from a Local IdP is treated, with regard to remuneration, in the same manner as a standard user creation.

5.2 Technical requirements for Local IdP

Tekniske krav til API integrationer mellem Lokal IdP'en og MitID Erhverv samt relateret dokumentation fremgår af hjemmesiden for MitID Erhverv:

Technical requirements for API integrations between the Local IdP and MitID Erhverv as well as related documentation can be found on MitID Erhverv:

https://mitid-erhverv.dk/en/advanced-functionalities-in-mitid-erhverv/mitid-erhverv-integration-test-environment/

The integration between NemLog-in and the Local IdP must comply with the OIOSAML Local IdP Profile, as described on the Agency for Digital Government's website:

https://digst.dk/OIOSAML

5.3 Maintaining Business Identities

The User Organisation is obliged to ensure that Business Identities are kept up-to-date in MitID Erhverv at all times and remain synchronised with the User Organisation's own records of Business Users, including ensuring that Business Identities are deleted when they are no longer required. This applies irrespective of the method of user creation used, cf. clause 5.

5.4 Issuing certificates and electronic signatures

5.4.1.Introduction

Business Users created and identity assured via a Local IdP may obtain the ability to create qualified signatures and qualified seals or OCES signatures and OCES seals via Den Danske Stat Signing Solution using identification means from the Local IdP either by 1) supplementary central identity assurance and user activation of Business Users via MitID Erhverv, cf. clause 5.4.2, or 2) on the basis of local identity assurance and user activation with the Local IdP, cf. clause 5.4.3.

5.4.2.Central identity assurance via MitID Erhverv

Business Users shall, on the basis of supplementary identity assurance with private MitID in MitID Erhverv, be granted access to create qualified signatures and qualified seals via Den Danske Stat Signing Solution using authenticators from a Local IdP.

5.4.3.Local Identity Assurance with the Local IdP

5.4.3.1.ACCESS TO ISSUING QUALIFIED SIGNATURES AND QUALIFIED SEALS

The User Organisation shall, on the basis of local identity assurance and user activation, have access to issue qualified signatures and qualified seals via Den Danske Stat Signing Solution using authenticators from a Local IdP, provided the Local IdP has obtained an eIDAS conformity assessment in relation to ETSI TS 119 461 at the level LoIP Extended.

The conformity assessment report must be addressed to the Danish eIDAS supervisory authority, with a copy to the Agency for Digital Government. The report must explicitly stated in the report that the assessment has been carried out for the purpose of documenting registration processes with a view to enabling the issuance of qualified signatures and seals.

Any costs incurred by the User Organisation in relation to local identity assurance, including requirements under this Annex 7, are of no concern to the Agency for Digital Government.

Upon expiry of a conformity assessment report, a new report must be submitted no later than 60 days following the date of expiry.

5.4.3.2.ACCESS TO ISSUING OCES SIGNATURES AND OCES SEALS

The User Organisation shall, on the basis of local identity assurance and user activation, have access to issue OCES signatures and OCES seals via Den Danske Stat Signing Service using authenticators from a Local IdP, provided the Local IdP has submitted an NSIS notification.

The User Organisation's costs relating to local identity assurance, including requirements under this Annex 7, are of no concern to the Agency for Digital Government.

Upon expiry of a conformity assessment report, a new report must be submitted no later than 60 days following the date of expiry.

5.4.3.3. AUDIT

When applying local identity assurance, the User Organisation must, upon reasonable notice and without remuneration, submit to an audit conducted by the Agency for Digital Government or by the Agency's conformity assessment body. The audit shall concern only matters relating to local identity assurance and shall therefore not extend to the User Organisation's other business or activities. The User Organisation is obliged to cooperate fully and in good faith in the audit and to assist in its completion. All communication with the conformity assessment body shall take place in English, and any relevant documentation must likewise be provided in English.

6.Provision of Full Service Local IdP

A User Organisation that is NSIS-registered as an Electronic Identification Scheme and Identity Broker, or has obtained an eIDAS conformity assessment in relation to ETSI TS 119 461 LoIP Extended may make its Local IdP available to other User Organisations, thereby acting as a FullService Local IdP in accordance with clause 4. The User Organisation determines its own agreements with such User Organisations using the FullService Local IdP.

The Agency for Digital Government may require the submission of special declarations in connection with the provision of a Full Service Local IdP.

7.Identity Assurance of Business Users

The User Organisation is responsible for ensuring that the Local IdP correctly validates the identity of the User Organisation's Business Users.

Requirements for identity assurance and derived Assurance Levels are specified in the NSIS and ETSI TS 119 461.

If an NSIS registered User Organisation verifies the identity of the natural person based on MitID, the overall Assurance Level for the Business User will correspond to the maximum NSIS Identity Assurance Level for the MitID in question

8.Responsibilities of the User Organisation

The general responsibilities of the User Organisation are regulated in the Terms and Conditions for User Organisations.

The User Organisation's liability related to the handling of local identities, Authenticators and authentications follows NSIS, including the requirements of NSIS clause 7.3 (Liability and Insurance).

The above stated responsibilities are independent of whether the User Organisation uses a Local IdP according to Model 1 or Model 2.

9.Ongoing maintenance of NSIS notification or eIDAS conformity assessment and revision

The NSIS notification or eIDAS conformity assessment referred to in clause 4 must be maintained on an ongoing basis in respect of the Local IdP in use, and the requirements set out in NSIS or ETSI TS 119 461 must be complied with on a continuous basis, including as regards audit.

Should the NSIS notification or eIDAS conformity assessment for the Local IdP in use cease to be maintainable for whatever reason, the User Organisation must immediately discontinue its use and deregister the Local IdP in MitID Erhverv.

The Agency for Digital Government shall be entitled to suspend access to the Local IdP if it no longer appears on the NSIS positive list or if it is established that a valid eIDAS conformity assessment is no longer in place

10. Ongoing Maintenance of the Basis for Issuance of Certificates and Creation of Signatures

The auditor's declaration or conformity assessment referred to in clause 5.4.3 must be maintained on an ongoing basis for the Local IdP in use if the right to create qualified signatures and seals is to be retained.

Translate into british english: Digitaliseringsstyrelsen kan (og vil i henhold til eIDAS være forpligtet til) uden varsel lukke for adgang til at afgive kvalificerede signaturer og kvalificerede segl eller OCES-signaturer og OCES-segl via Den Danske Stat Signeringsløsning, såfremt Brugerorganisationen ikke rettidigt leverer den i punkt 5.4.3 anførte revisionserklæring eller overensstemmelsesvurderingsrapport.

Similarly, the Danish Agency for Digital Government may, without prior notice, suspend access to the creation of qualified signatures and seals via Den Danske Stat Signing Solution if an audit or conformity assessment identifies material deficiencies, or if such deficiencies are identified on the basis of an audit. The Danish Agency for Digital Government is likewise entitled to suspend access to the creation of qualified signatures and seals if the Local IdP fails to cooperate loyally in the audit.

The auditor's declaration or conformity assessment referred to in clause 5.4.3 must be maintained on an ongoing basis in respect of the Local IdP in use if the right to issue qualified signatures and qualified seals or OCES signatures and OCES seals is to be retained.

The Agency for Digital Government may (and, pursuant to eIDAS, will be obliged to) suspend, without prior notice, access to the issuance of qualified signatures and qualified seals or OCES signatures and OCES seals via Den Danske Stat Signing Solution if the User Organisation fails to submit, in due time, the auditor's declaration or conformity assessment report referred to in clause 5.4.3.

Similarly, the Agency for Digital Government may, without prior notice, suspend access to the issuance of qualified signatures and qualified seals, or OCES signatures and OCES seals, via the Den Danske Stat Signing Solution, should an audit or conformity assessment identify material deficiencies, or should such deficiencies otherwise come to light through an audit. The Agency for Digital Government is likewise entitled to suspend access to the issuance of qualified signatures and qualified seals, or OCES signatures and OCES seals, should the Local IdP fail to cooperate fully with the audit.

11. Notice of cessation or deregistration

Upon termination or deregistration of a Local IdP or Full Service Local IdP, the User Organisation is obliged to notify the MitID Erhverv of the reason for such termination or deregistration. The User Organisation is likewise obliged to submit a final declaration covering the period that has not yet been audited.

Annex A Management declaration on the use of FullService Local IdP

Annex A is set out below and may be downloaded from:

mitid-erhverv.dk/ledelseserklaering

Bilag A – Ledelseserklæring om anvendelse af FullService Lokal IdP

CVR-nummer på Brugerorganisationen* (8 cifre uden mellemrum):

Navn på Brugerorganisationen:

Navn på ledelsesrepræsentanten i Brugerorganisationen*:

E-mailadresse på ledelsesrepræsentanten i Brugerorganisationen:

Navn på leverandørens FullService Lokal IdP:

CVR-nummer på leverandøren af FullService Lokal IdP (8 cifre uden mellemrum):

På tro og love erklærer undertegnede ledelsesrepræsentant for Brugerorganisationen følgende:

- At undertegnede varetager en rolle som ledelsesrepræsentant for Brugerorganisationen og kan forpligte denne i forhold til denne ledelseserklæring og de tilhørende vilkår for tilslutning af Lokal IdP.
- Brugerorganisationen ønsker at tilknytte ovenstående Lokal IdP til Brugerorganisationen efter modellen FullService Lokal IdP med henblik på, at Brugerorganisationen kan anvende denne til autentifikation af lokale brugere i sammenhæng med MitID Erhverv.
- Ved identitetssikring af brugere og udstedelse af identifikationsmidler baserer Brugerorganisationen sig udelukkende på den service og de processer, der er udføres af den valgte FullService Lokal IdP, og som er indeholdt i revisionen heraf, og som danner grundlaget for NSIS-anmeldelsen for Lokal IdP'en.
- Brugerorganisationen varetager ikke opgaver eller udfører aktiviteter reguleret af NSIS i tilknytning til den anvendte FullService Lokal IdP, herunder registrering eller identitetssikring af brugere.
- Det sikres, at eventuelle øvrige lokale IdP'er Brugerorganisationen opretter enten er dækket af en selvstændig ledelseserklæring om anvendelse af FullService Lokal IdP eller er tilknyttet Brugerorganisationen selv, og er NSIS-anmeldt.
- Denne ledelseserklæring anvendes alene som grundlag for tilslutning af ovenstående Lokal IdP. Såfremt Brugerorganisationen ønsker at anvende øvrige FullService lokale IdP'er tilsluttet MitID Erhverv, sikrer Brugerorganisationen, at der afgives en separat ledelseserklæring herom.
- Brugerorganisationen er i det hele ansvarlig for de services, der udføres af Lokal IdP'en og påtager sig et ansvar svarende hertil over for Digitaliseringsstyrelsen og øvrige parter.
- På Brugerorganisationens vegne indestår jeg for, at ovenstående oplysninger er korrekte, og at jeg i øvrigt er bekendt med vilkår for Lokal IdP udarbejdet af Digitaliseringsstyrelsen.

Dato*:
(dd.mm.åå)

Ledelsesrepræsentantens underskrift*:
Indsæt underskrift, fx ved at anvende Adobe Acrobat Readers Udfyld og Underskriv-funktion.
Ellers udskriv, skriv under i hånden og scan.