DANISH AGENCY FOR DIGITAL GOVERNMENT

Erhverv

Annex 7
Terms and conditions for use of Local IdP

Content

Annexes

Annex A Management declaration on the use of Full-service Local IdP

1 Introduction

These Terms govern a User Organisation's use of a Local IdP with MitID Business.

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.
- 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 Forvaltningen
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 review and compliance

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.

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 notifies its own Local IdP and is subject to the audit required by the NSIS standard, including 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.

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

Under Model 1, the User Organisation appears on the NSIS positive list regardless of whether the User Organisation is NSIS notified alone or is covered by a joint notification.

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 and handles all technical and procedural matters regulated in NSIS including registration and identity assurance of users and issuance of Authenticators. The external Full-service Local IdP is subject to the audit required by the NSIS standard. Under Model 2, the third party appears in the NSIS Positive List.

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 Forvaltning, cf. clause 2.

The management declaration can also be downloaded from www.mitid-erhverv.dk/avanceret/lokal-idp/dokumentation

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).

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
- Via IdM API interface exposed by MitID Erhverv

5.2 Technical requirements for Local IdP

Technical requirements for API integrations between the Local IdP and MitID Erhverv as well as related documentation can be found in the pre-production environment for User Organisations: www.nemlog-in.dk/vejledningertiltestmiljo/

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/it-loesninger/standarder/oiosaml-profiler/

5.3 Maintaining Business Identities

The User Organisation is obliged to ensure that Business Identities are always up-to-date in MitID Erhverv and synchronised with the User Organisation's own records of Business Users. This applies irrespective of the method of user creation used, cf. clause 5.1.

5.4 Issuing certificates and electronic signatures

Issuance of qualified signatures and qualified seals via the by Den Danske Stat Tillidstjenester (The Danish State's Trust Services) Signing Solution using an Authenticator from a Local IdP requires the Business User to undergo additional identity proofing with a private MitID in MitID Erhverv.

6 Provision of Full Service Local IdP

A User Organisation that is NSIS-registered as an Electronic Identification Scheme and Identity Broker may make its Local IdP available to other User Organisations, thereby acting as a Full Service Local IdP in accordance with clause 4. The User Organisation determines its own agreements with such User Organisations using the Full Service 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 standard.

If the User Organisation verifies the identity of the natural person on the basis of NemID or MitID, the overall Assurance Level for the Business User will correspond to the maximum NSIS Identity Assurance Level for the NemID or 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 the NSIS standard, including the requirements of NSIS Section 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

An NSIS notification must be maintained for the Local IdP used and the requirements of the NSIS standard must be continuously complied with, including in relation to auditing.

If the NSIS notification for the Local IdP used - for whatever reason - cannot be maintained, the User Organisation must immediately cease using it and deregister the Local IdP in MitID Erhverv.

10 Notice of cessation or deregistration

The User Organisation is obliged to inform the MitID Business Administration of the reason for the termination or deregistration of a Local IdP.

Annex A Management declaration on the use of Full-service Local IdP

Management Statement on the use of Full-service Local IdP

CVR no*:	[Insert User Organisation's CVR number]
User organisation	[Insert name of User Organisation]
Name*:	[Insert name of Management Representative]
E-mail address:	[Insert email address of Management Representative]

Local IdP	[Insert name of Full-service Local IdP]
CVR number:	[Insert CVR number of the Provider of the Local IdP]

I, the undersigned Management Representative of the User Organisation, declare on my word of honour that:

- The undersigned is acting in the capacity of a Management Representative of the User Organisation and can commit to this management declaration and the associated terms and conditions for joining the Local IdP

- The User Organisation wishes to associate the above stated Local IdP to the User Organisation according to the Full-service Local IdP model in order for the User Organisation to use it for authentication of local users in the context of MitID Erhverv.

- In securing the identity of users and issuing Authenticators, the User Organisation relies solely on the services and processes performed by the Local IdP and contained in its audit, which form the basis of the NSIS notification for the Local IdP.

- The User Organisation shall not perform any tasks or activities regulated by NSIS in connection with the Local IdP, including registration or identity proofing of users.

- This management declaration is used solely as a basis for connection of the above stated Local IdP. If the User Organisation wishes to connect other full-service Local IdPs to MitID Erhverv, a separate management declaration is required.

- The User Organisation is responsible for the services provided by the Local IdP and assumes a corresponding responsibility towards The Agency for Digital Government and other parties.

- On behalf of the User Organisation, I warrant that the above information is correct and that I am familiar with the terms for Local IdP prepared by the Agency for Digital Government.

Date: [...]

Signature: [...]