DIGITALISERINGSSTYRELSEN

The future infrastructure for digital identities in Denmark

In the course of the coming years, Denmark's digital infrastructure will be rebuilt.

At the end of 2017, parallel invitations to tender will be published for the next generation of NemID (MitID) and NemLog-in (Nemlogin3). Some features will continue, while others will be changed completely. The vision across the tender procedures is to create long-term solutions with a high degree of flexibility and positive user experiences. Here, we give you the big picture of the solutions that will come to shape the future infrastructure for digital identities, signing and user rights management in Denmark.

Content

MitID tender

Background
The Danish Agency for Digitisation and Finans Danmark have, through the subsidiary FR1 AF 16. SEPTEMBER 2015 A/S ('FR1') entered into a partnership on the joint development and operation of MitID, which is a new, central identity provider for digital personal identities. The solution will be put out to EU tender at the end of 2017 and will replace NemID.

MitID will build on one common identity core. This core may be used by public players as well as financial institutions and other private service providers with a need for secure digital personal identities. One of the main objectives is that all personal identities in the core may basically be used across sectors and service providers, no matter which player registered and enrolled the person in question.

Scope
The financial and public sectors have different requests for the solution, for instance in respect of authorisations, powers of attorney, document signing and approval of transactions. Therefore, the focus of the MitID tender will be on the parts of the future identity solution where the two sectors have common needs. The other elements will be developed separately by the individual parties.

The predecessor, NemID, which is operated by Nets DanID A/S, consists of two independent parts: the 'banking solution' and the public, PKI-based 'OCES solution'. The new partnership will end this division. The focus of the MitID tender will be to develop a common identity and authentication solution with an identity core that supports authentication and life-cycle handling of digital personal

DIGITALISERINGSSTYRELSEN

identities. Life-cycle handling includes process and system support for, e.g., registration, enrolment, updating and blocking of personal identities and credentials (login devices).

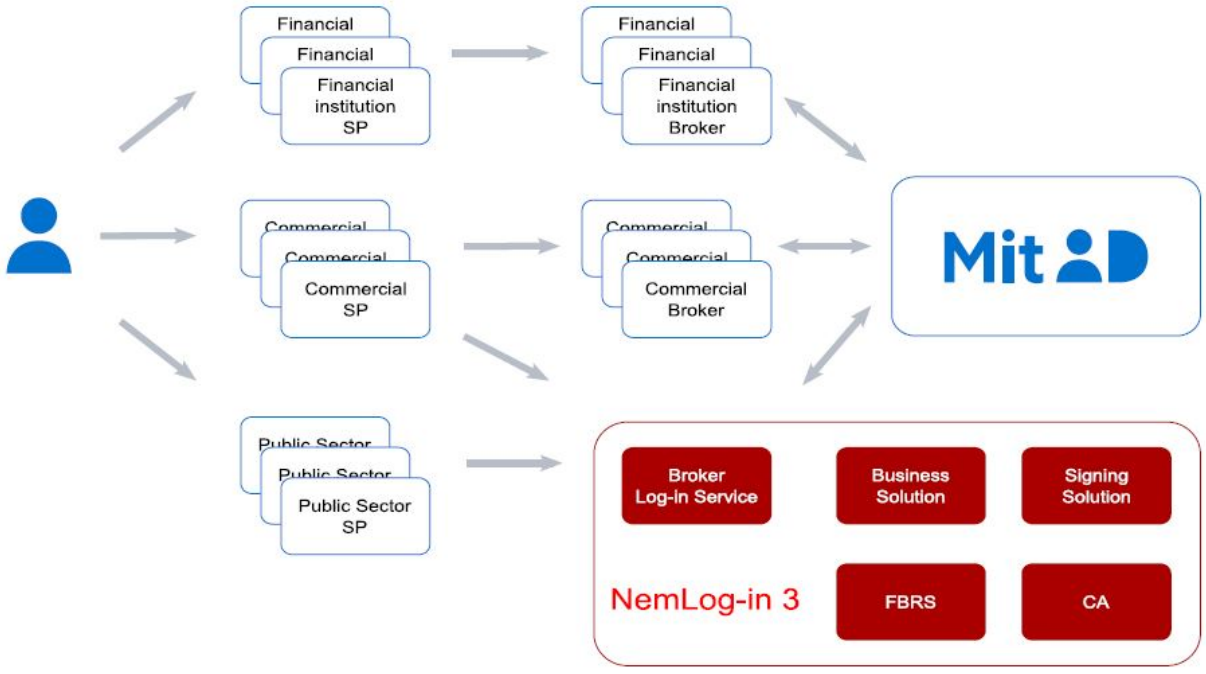
For users, a set of standard credentials must be developed that can be expanded on an ongoing basis in line with the general technological and business development. As a minimum, a smartphone-based authentication factor, a password-based authentication factor and a physical authentication factor will replace the NemID code card. Credential support of special needs will also be a requirement, for instance for frequent users who need to authenticate themselves many times a day, and users with disabilities.

The transition from NemID to MitID will entail a number of changes to the infrastructure:

- MitID personal identities are no longer necessarily certificate-based (PKI).
- Document and transaction signing is not a part of the MitID core, but must be handled individually by MitID buyers' own solutions.
- A new solution to replace NemID's identity provider of employee identities (NemID employee signature) is not part of the MitID core but will be offered by the Danish Agency for Digitisation as a sub-project under the NemLog-in3 call for tender.
- The MitID core will be developed so that external parties, so-called 'identity brokers' (brokers), can provide their own client solutions with end-user authentication via the MitID core.

Compulsory use of identity brokers

The MitID infrastructure will generally no longer allow ordinary service providers (SPs) to join the core directly. Instead, they must go through a certified identity broker that handles the actual authentication process for the end user and the underlying technical integration to the core. The broker acts as proxy identity provider between the SP and MitID and issues its own authentication ticket for the SP in, e.g., SAML format. Alternatively, the SP may itself enter into a broker agreement with MitID, which, however, will imply significantly stricter safety requirements compared with, e.g., the existing NemID service provider agreement.



DIGITALISERINGSSTYRELSEN

In the existing identity infrastructure, the vast majority of public service providers are connected to the NemID solution via the joint public login portal/identity broker, NemLog-in, and a number of private SPs also use similar commercial solutions rather than having to implement the NemID client in their own online solutions via the so-called 'NemID SP package'.

One of the major advantages of the broker model is that the individual SP does not have to consider the technical integration to the underlying identity provider. Instead, they may connect with the selected broker against an often simpler interface, which is typically based on international open standards. This also means that only broker players need to consider changes in MitID interfaces and safety procedures etc.

It is expected that three different categories of identity brokers will provide services to SPs in different sectors. These include brokers for the public sector (NemLog-in and others, if any) as well as brokers for individual banks or bank data processing centres and, finally, commercial brokers for SPs from other parts of the private sector. The core provides brokers with a client[1], but each broker may implement its own client for authentication via the core and may thus extend or adapt the functionality as required.

EU legislation
One of the areas that has developed significantly since the introduction of NemID is the European Union legislation governing the area.

The eIDAS Regulation
For the public sector, the eIDAS Regulation is of special importance. This regulation defines requirements and standards for the national, public self-service solutions, permitting the use of digital identities across EU member states. From 18 September 2018, public SPs in all EU countries are obliged to receive and acknowledge official, digital identities from other EU countries in line with the country's own digital identities.

Denmark expects to report MitID as a national eID solution so that identities from MitID are recognised across the EU. The Danish Agency for Digitisation has prepared a National Standard for Identity Assurance Levels (NSIS), which defines the requirements applying to Danish eID solutions to ensure that they live up to the eIDAS Regulation's three assurance levels (or LoA – Levels of Assurance) for digital identities. In the future, all public SPs, brokers and identity solutions using the national infrastructure must comply with this standard when they develop new services. The data which can be accessed through these services must be protected with authentication at a sufficiently high assurance level.

Payment Services Act
From 2018, a number of new requirements will be introduced for the financial sector with the revised Payment Services Directive (also called PSD2). Among other things, the Directive includes detailed requirements as to the authentication and transaction approval in connection with the provision of payment services, e.g. payments via online banking. The parties behind the FR1 will all have to live up to these rules through the Danish Revised Act on Payments, which enters into force on 1 January 2018. Thus, MitID will support such regulatory requirements.

---

[1] A client is the part of MitID which presents a login prompt for end users and handles communication with the MitID core.

DIGITALISERINGSSTYRELSEN

General Data Protection Regulation
From 2018, a new regulation on the protection of personal data (GDPR) will come into force. The GDPR regulation will impact all public and private services that handle personal data, i.e. also MitID. The GDPR is more far-reaching in its operational requirements for players than the previous regulation, and sanctions are considerably larger.

Registration authorities
Personal identities will be registered in the MitID core in more or less the same way as today. However, minor adjustments will be made to ensure that the registration processes live up to the requirements defined by the NSIS standard. For further information, please see the Danish Agency for Digitisation's guide to the NSIS standard.

MitID will support the registration of personal identities up to the highest NSIS assurance level (4/high). It is expected that the majority of the personal identities will in future be registered according to the NSIS assurance level 3 (substantial).

In the same way as the existing NemID solution, players will be appointed to act as registration authorities (RAs) with the option to create new personal identities in the solution. Depending on the assurance level required by the individual registration authorities for the registration of personal identities, the players must live up to a number of requirements.

Looking forward, public authorities acting as points of contact for citizens, e.g. municipal citizens services centres, prison authorities and refugee authorities, will probably also function as RAs in the future.

In relation to end-users who are using MitID in a business context, NemLog-in3 will offer a registration portal as part of the future business identity solution.

Private actors may also be certified to perform the role as RA up to an optional NSIS assurance level (certification requirements will reflect the requested assurance level). This could be financial institutions solving a similar task in the current NemID, or other private players from other sectors in society.

MitID will also be able to automate registration processes online, allowing end-users to register and enrol on the lower assurance levels (up to NSIS assurance level 3) without personally appearing before an RA.

MitID in a joint public context
With the introduction of MitID, the public strategy is to continue to develop along the lines of a more flexible and modular architecture in the public-sector infrastructure for digital identities, signing and user rights management.

From a service provider's perspective, the NemLog-in solution will play an even more central role in the future infrastructure than it does today. One of the reasons for this is that, in the future, NemLog-in acting as MitID broker will be the primary access point for the identity infrastructure for public services.

At the same time, the NemLog-in solution is expanded with a new identity provider and administration portal for business identities as a supplement to the MitID core. In this way, all the

essential functionality parts are gathered around business identities and their administration in NemLog-in. The aim is to create a more coherent user experience for business users and company administrators. In the future, user administration and rights administration are handled in one place. At the same time, the flexible and modular infrastructure specified for both MitID and NemLog-in provides better opportunities for using functionalities across the two solutions. One of the specific objectives is to give business users the opportunity to use the same types of credentials in a business context as in a private context.

MitID in a financial sector context
Finans Danmark will, in cooperation with the Danish Agency for Digitisation, solve the task of providing the Danes' future digital identity solution. Finans Danmark is the interest organisation of banks, mortgage credit institutions and asset managements in Denmark and handles among other sector- and digitised infrastructure projects across the financial institutions.

The digital development in Denmark has been widely supported by a unique trinity of well-developed public self-service solutions, a digital and safe payment infrastructure and a high level of data quality and safety for users through a digital identity, bound by the Danish civil registration number (CPR), in the form of NemID. With the introduction of MitID, the financial sector wants to continue to solve this task of national importance by using modern and user-friendly interfaces that ensure a frequent and safe use, along with a dissemination of the Danes' digital everyday life. MitID has also made it possible to formalise an existing operational cooperation, and FR1 shares the joint public-sector vision of a more flexible and modular architecture in the joint public-sector infrastructure in order to not only optimise the user experience, but also toward streamlining the continuous exchange of data between public and private players.

In parallel to the common interest in the digital infrastructure, the financial institutions are guarantors of a constantly competitive and modern development of the broker infrastructure aligned with MitID. The financial sector will expectedly develop a number of broker solutions to support the underlying and sometimes proprietary banking solutions where the individual customer experience will continue to vary in-between financial institutions.

Depending on the specific context, the technical requirements for the authentication process will therefore vary from broker solution to broker solution. This is reflected in the MitID architecture by specifications that allow it to be used via several different models with various degrees of flexibility for the players acting as identity brokers in the MitID infrastructure.

PKI/CA functionality
Unlike the current NemID solution, the MitID core must not be based on certificate-based (PKI) identities. The OCES certificate portfolio will not be discontinued, but it is expected that the policies are revised and adapted to future needs. This means, among other things, that:

- The future Certificate Policies (CP) instead of the current DS-844 standard will be based on the corresponding ETSI standard (319 411).
- The requirements for OCES individual and employee certificates (POCES and MOCES) are intensified, so that the certificates will in future consist of qualified certificates instead of non-qualified certificates.
- New customised certificate policies/certificate profiles are created for signing via single-use certificates with MOCES /POCES.

DIGITALISERINGSSTYRELSEN

- The MOCES infrastructure is adapted so that there is no longer support for locally installed key files in software on the PC and the like. MOCES will only support decentralised solutions that offer hardware-based protection of private keys, e.g. a central signature server or equivalent. This is done to ensure a uniform substantial or high assurance level for PKI-based authentication.
- CP for FOCES and VOCES is expected to be updated so that RA-specific X.509 V3 attribute extensions are supported.

Migration of users from NemID to MitID
Together with the supplier of the coming MitID, a plan must be prepared for migrating personal identities from NemID to MitID. In order to ensure a high rate of dissemination of MitID and to reduce any inconvenience for the individual end-user, the migration process must be performed as smoothly as possible. It is not expected, however, that all existing NemID identities can be transferred to MitID on a 1:1 basis. Read more below about migration of business identities.

NemLog-in3 tender

Background
NemLog-in plays a central role in Denmark's digital infrastructure by making it possible for Danish citizens and businesses to log into public self-service solutions. The Danish Agency for Digitisation wishes to continue and further develop the NemLog-in, which requires that the solution is put out to a new tender, as the contract with the current supplier, NNIT A/S, expires in 2019. In addition, a business solution will be developed in cooperation with MitID.

The NemLog-in3 project is carried out via two tenders:

- An invitation to tender for the operation of the project
- An invitation to tender for the development and administration of the project.

Below, references to the project covers both tenders. Find an overview of the division between the two tenders on page 12.

Overall scope
NemLog-in is continued and will continue to function in the same roles as today. It will therefore be the primary joint identity broker/IdP solution and integration point for public SPs and self-service solutions and offer the same range of services as is the case today. This includes, e.g., the login portal with Single Sign On (SSO) functionality, central user rights management (FBRS), signing service (incl. signature validation and possibly long-term storage), power of attorney functionality and Security Token Service (STS) functionality.

The functionality already offered by NemLog-in in the existing infrastructure for public SPs is not expected to be changed fundamentally. On the other hand, there will be a number of expansions with new functionality as well as adjustments of the existing functionality.

The main additions will be:

- A new business identity provider will be created, including an administration portal for business identities to replace the OCES-based 'NemID employee signature' solution.

DIGITALISERINGSSTYRELSEN

- The CA functionality (OCES) which in the current infrastructure is supplied as part of NemID, will in future become part of the scope of the NemLog-in3 tender.
- The signing solution will be upgraded and modernised significantly in relation to new signing standards etc.

Another major change is that relevant private SPs will expectedly be able to use parts of the NemLog-in infrastructure.

In relation to existing components, the following changes, among others, will be made:

- The NemLog-in login portal will be updated so that it supports authentication via MitID.
- FBRS will be updated so that the component is better integrated with the future business identity solution.
- The current power of attorney component will be updated to support future needs and become more user-friendly.

Below is a short review of the most important NemLog-in components and their role in the future infrastructure.

Login portal with Single Sign On
NemLog-in's existing login portal will be updated in order to support authentication via MitID. It will only to a lesser extent impact existing SPs, as the current SAML interface as far as possible is maintained. Some attributes in the current interface cannot be maintained since they are closely connected to OCES certificates. NemLog-in will become a broker solution in relation to the MitID infrastructure and will serve as the primary point of entry for public SPs with unchanged functionality in relation to Single Sign On (SSO). Moreover, the portal is also expected to be used by private SPs to connect with the MitID infrastructure.

In addition to private personal identities from MitID, the login portal will also support authentication of business identities. Depending on the preferences of business users (and the organisation), business users will either be able to authenticate themselves via a business identity coupled to the private MitID credentials or via dedicated business credentials. As described below, the latter will either come from MitID or be MOCES PKI-based credentials. Hence, a looser coupling between business identities and credentials, than is the case today, will be introduced to grant a more flexible infrastructure and user experience.

If the user has attached its private MitID credentials to one or more business identities, the login portal will be responsible for determining in which context, in the specific session, the user is going to operate. The SAML authentication ticket passed on to the SP will therefore vary, depending on whether the user chooses to act as a private individual or as an employee. From March 2017, this functionality has already been partially implemented in the NemLog-in login portal in the so-called 'NemID Private to Business' solution, where fully liable partners and other persons with full rights to sign for a company can log in as employees with their personal NemID.

In the long term, NemLog-in is planned to act as a broker for local Identity Providers (idP) – regulated within the framework of the NSIS standard. The idea is to realise this by opening up for federation between NemLog-in and other IdPs. This allows for authentication with other credentials

DIGITALISERINGSSTYRELSEN

than MitID credentials – e.g. locally issued credentials in an organisation exhibited through an Identity Provider.

Signing in the future infrastructure
A signing component based on the CEN standard for Remote Signing (CEN EN 419 241) will be developed and expectedly published at the end of 2017. The component will be constructed as part of the NemLog-in3 tender to integrate it in the best possible way with the existing signing service in NemLog-in.

Signing will be based on end-user authentication via the MitID core or other identity provider, e.g. NemLog-in3 for business identities. The component is expected to support the signature formats PAdES and XAdES as well as other requested signing document formats. As opposed to the existing solution, it will be based on qualified single-use certificates that will be issued by the infrastructure's CA component. Using qualified certificates in the signing service gives the advantage that commercial standard products such as Adobe PDF Reader will be able to verify the validity of signed documents directly without the use of special tools.

The future business solution
To replace the NemID employee signature, NemLog-in3 will include a completely new identity provider for business users.

This business identity provider will handle the full life cycle of business identities and be designed so that it can be integrated with MitID, if applicable.

In relation to business user credentials, the business solution will offer four types of access:

1. Automatic coupling between private personal identity/credentials and companies where the person can sign for the company alone. This is the solution which was put into operation with NemID from March 2017.
2. A dedicated business identity where a relationship between the person's private MitID and CVR numbers is registered for the companies/organizations to which the person is associated (mapping between MitID and CVR number).
3. A dedicated business identity with associated credentials, created in MitID. These credentials may be shared between several business identities or may be dedicated to one specific business identity.
4. MOCES PKI-based credentials (key pair with OCES certificate).

In relation to item 2, there will be a double principle of voluntariness so that this option will only be available if both the employee and the company accept authentication via the employee's private MitID credentials.

A central component in the business solution will be a portal for companies where the company's administrator will be able to administer the employees' business identities and the related roles and rights that have been created in the FBRS component.

Joint conclusion of agreement for companies across systems
In order to reduce the administrative burdens for companies, an effort is made to provide joint conclusion of agreements for companies across the joint public-sector infrastructure solutions NemLog-in, MitID and Digital Post. Instead of entering into individual user agreements with the

individual infrastructure solutions, the plan, looking forward, is to conclude only one agreement and, if possible, to do it digitally.

Registration authorities in the business solution
Companies and other organisations with an associated CVR number will still have the possibility of creating employee identities as with the previous administrator role in the NemID employee signature. However, there will be a change in relation to maintaining the assurance levels for personal identities defined with the NSIS standard. Companies will, as a general rule, only be able to issue business identities to their employees at the NSIS level of security to which they can be certified. Subsequently, it will be possible to raise the assurance level for such an identity letting the employee validate his or her identity using his or her private personal identity (or another personal business identity).

If the company and/or the employee wants to use MOCES credentials, the business solution will facilitate the creation of the MOCES certificate in the infrastructure CA component.

Common user rights management
A central component in the existing NemLog-in solution is the common user rights management component (FBRS). It acts as a user administration component for a wide range of public services and online solutions aimed at businesses. Today, FBRS is based on the ID key (RID) found in the NemID employee signature solution. Via the FBRS administration portal, companies and organisations can administer rights in a common portal across connected online solutions for all the employees created by the company in the NemID employee signature solution.

The FBRS solution currently covers approx. 250,000 companies and organisations. If employees from these companies authenticate themselves via the NemLog-in portal, all relevant rights are automatically included as part of the authentication ticket for the individual solution.

In the future infrastructure, FBRS will be more closely integrated in the future business identity provider replacing the NemID employee signature.

In order to improve the user experience for administrators in companies and organisations alike, FBRS will be updated in a number of ways. First of all, it will be service-enabled so that rights can be administered from external systems via API, and a new customer administration portal will be set up to give businesses or organisations a more intuitive portal for handling business identities and related rights.

Another planned expansion is that FBRS must be able to handle more detailed rights in the form of data restrictions as a supplement to the existing static roles.

Migration of users from the 'NemID employee signature' to the future business identity provider
All existing business identities in the NemID employee signature are basically expected to be migrated to the new business solution, so that the individual company does not need to establish new rights for its business identities (employee identities) in FBRS and any other external systems. A change in relation to this will be that the migrated business entities will need to be classified at an NSIS level of security which will depend on the registration process for each business identity.

Migration in NemLog-in covers a number of activities with a certain flexibility in relation to time, but also with links and dependencies, e.g. to specific milestones in MitID. The following migration activities are found:

- Companies must conclude agreements on the connection to the NemLog-in's system for handling business identities.
- Data about who is appointed as NemID administrators must be transferred from the current NemID employee signature solution.
- Business identities must be migrated from the current system to NemLog-in. Here, it must be ensured that related data (e.g. rights in FBRS) retain their relation to business identities.
- Certificate-based (OCES) identities must be replaced by new corresponding identities created in the new CA under the revised certification policy.
- Business identities that will not be associated with OCES credentials (private key + certificate) will have to be associated with MitID credentials instead of the current NemID credentials.

Access to MitID and the NemLog-in infrastructure for private service providers
To ensure that private SPs will also in future have access to the services available in the national eID infrastructure (e.g. authentication of users), an effort is made to provide access for this group of SPs via an identity broker solution under the auspices of NemLog-in.

Depending on the interest from the private market in relation to stepping into the role as identity broker in MitID for private SPs, it is likely that, over time, other access points than the NemLog-in described above will be offered.

The eIDAS Gateway for integration with other national eID solutions from the rest of the EU
As described above, public service providers will, from 2018, be obliged to recognise digital identities from other EU countries, provided that these are eIDAS-notified identity solutions. This means that public service providers must support authentication with credentials from other countries' eIDAS-notified identity providers.

To be able to administer this setup the Danish Agency for Digitisation establishes a so-called 'eID Gateway' to administer identities from other EU countries' national identification solutions, and transform these into a format that can be used by Danish public self-service solutions. The gateway will offer a SAML-based interface to Danish service providers which, as far as possible, resemble the existing OIOSAML interface in NemLog-in, in order to let the services reuse their existing integrations extensively.

Migration of service providers to the future infrastructure
Depending on how service providers currently use the existing NemID solution, migration to the future infrastructure can be either a major or a minor task. This all depends on whether the SP integrates directly with NemID using the SP package, or whether the SP uses an intermediate identity broker solution as, e.g., NemLog-in or NemAdgang. In the latter case, the task for the individual service provider could be minimised, as migration-related changes can largely be limited to the broker level, so that the SP can continue with an unchanged (or minimally altered) interface to the infrastructure.

As the future infrastructure will be offered on other terms than the existing NemID solution, it is expected that all private service providers will enter into new agreements to be able to use MitID. Depending on how the individual identity broker chooses to handle integration with MitID, there may be certain derived consequences in the form of interface changes for the related SPs etc.

DIGITALISERINGSSTYRELSEN

Ownership of the joint public-sector infrastructure
In order to make it possible to further develop existing solutions and create closer integration between solutions, it is a goal for the future joint public-sector digital solutions, including NemLog-in3, MitID and Next Generation Digital Post, to obtain a high degree of rights and ownership.

The Danish Agency for Digitisation also wants to be able to use commercial standard components to avoid having to develop a standard functionality from scratch in the joint public-sector systems, and to ensure that the public sector will not bear the full cost of the ongoing maintenance of, e.g., source codes.

For all parts of future solutions that have not already prior to the individual tender procedures been developed as standard components and used by a wide range of customers, suppliers will be required to have full rights to an extent that allows for unlimited further use, operation and development – even after the expiry of the contracts.

The scope of the coming tenders

In closure, a summary is provided of the expected scope of the invitation to tender concerning MitID and the future NemLog-in solution, respectively.

Scope of MitID tender
In relation to the existing NemID, the following content in the solution is changed.

The scope of the tender is generally as follows:

- Development of identity provider and authentication solution for personal identities.
- Support for authentication and 'life-cycle handling' for digital personal identities considering different models for identity brokers and service providers.
- Facilitation of standard credentials for users of the solution.
- Operation, maintenance and further development of the solution.
- Process and system support for processes such as registration, enrolment, updating, barring etc. of personal identities and related credentials (login means) with focus on compliance in relation to security-related requirements.
- Facilitation of migration to MitID of users from NemID.

Read more on page 1.

NemLog-in3 is divided into two tenders
The scope of the coming NemLog-in3 solution will include a continuation of existing components in the NemLog-in solution.

In addition, the scope will be extended so that functionality and services which are currently handled by the joint public-sector part of NemID, but which in future will not be part of the MitID tender, will be continued under NemLog-in3. This applies, for example, to the 'NemID employee signature' PKI/CA, document signing functionality and support for private service providers' access to the MitID infrastructure.

DIGITALISERINGSSTYRELSEN

To be able to handle the internal and external dependencies identified to continue the NemLog-in solution in the best possible way, it has been decided to divide the future version of the solution in two separate tenders: An IT operation tender and a development and administration tender.

Scope of NemLog-in3, operation tender
The scope of this tender is to continue the operation of the various components in the existing NemLog-in solution as well as ongoing take-over and commissioning of new and/or updated components in the NemLog-in solution from the future NemLog-in development supplier.

Scope of NemLog-in3, development and administration tender
The scope of this tender is expected to consist of a number of development-related services and a number of more administration-related services.

Development-related services:

- Development of a business identity provider.
- Development of a new signing service.
- Further development of the functionality in the existing NemLog-in solution
- Implementation of new PKI/CA to continue the OCES certificate infrastructure.
- New development and further development in relation to the support of private SPs' access to the NemLog-in infrastructure.

Administration-related services:

- Administration, support and general support of public SPs' access to NemLog-in and the MitID infrastructure.
- Handling of obligations in relation to the role as identity broker in relation to MitID.
- Administration, support and general support of private SPs' access to NemLog-in and the MitID infrastructure
- Handling of obligations related to the role of the CA in relation to the future continuation of the OCES certification infrastructure.
- Responsibility for processes and collaboration in connection with further development, testing, release, commissioning, change requests, incident response management etc.