Agency for Digitisation
Ministry of Finance

The Next Generation of National Electronic Identity and Signing in Denmark

April 2016

The Next Generation of National Electronic Identity and Signing in Denmark

Landscape

Since its introduction in 2010, NemID has become an unparallelled success in the area of national electronic identification and signing systems. More than 92% of Danish citizens today use NemID to do online banking, interact with public sector self-service solutions and with various private third parties – and the field is expanding. NemID has become a very common brand and is unique in its wide application across all of these sectors. In many other countries these sectors each have their own individual identification, signing and log-in solutions.

Leading the Way

Denmark has long been a technological forerunner in the field of national electronic ID and signature infrastructure – with increased technological possibilities and maturity it is time for a fresh look at how a future identity and signing solution should look and how it could be built.

Critical Infrastructure

The popularity of NemID also means it has become a critical component in the digital life of the nation; the foundation on which an efficient and effective digital infrastructure has been built – and continues to expand. One of the biggest successes of NemID lies in the successful adoption by societal groups that are usually considered technologically challenged, foremost among them the elderly. First of all, this is a testament to the tenacious and curious elderly of Denmark, but also in large part a tribute to the system's relative ease-of-use and comprehensibility. And this is a vital part of the obligation of the public sector: Ensuring that everyone can take part is a basic precondition – so providing a seamless and easy user experience will play a large part in honouring this obligation.

Mobile

Over the past four years, smartphones and tablets have become mainstream along with high speed mobile internet connectivity, so to a large extent the future of any identity solution will be based on mobile use cases. Integrating authentication and signing into the mobile experience is a priority as society now moves into younger generations for whom their first and perhaps only Internet terminal is a smartphone – as well as an elderly generation that have embraced tablets in a big way.

Technological Maturity

As the field of electronic identification and electronic signatures has matured, technologies once ground-breaking are superseded by industry best practices and standardised tools, components and solutions. The next generation of the Danish national identity solution will only be made more robust and extensible if it is based on loosely coupled standardised or off-the-shelf components – and a field such as biometrics has also seen a growing maturity and adoption and might be considered as one type of credential to be used for authentication in a future solution.

New Horizons

From this vantage point, we can see some of the principles that will shape the next generation of the National Digital Identity and Signing (NDIS) solution in Denmark.

Cross-sectoral Cooperation

NemID is a solution shared by the financial sector and the public sector, even though it was not developed in concert. However the benefits of a shared solution are such that regarding the core functionality a close collaboration between the sectors is planned for the next version.

Single Strong Electronic Identity

A strong electronic ID with a high level of security is the centrepiece of any national digital strategy that includes legally binding self-service and a trusted digital communication service. These are services that already exist in Denmark, so the coming generation of NDIS must make continuity a vital metric. Flexibility in integrating with the existing systems landscape will be paramount, all the while allowing for new technological opportunities that will expand system versatility and user-friendliness.

Standardised and Off-the-shelf Components

Basing the next generation of NemID on loosely coupled and adapted industry standard components, open source solutions and commercial off-the-shelf components is expected to provide greater flexibility to the overall solution, agility in the on-going development cycle, and a faster response-time to the ever-changing landscape - technologically and legislatively.

Not Just Web

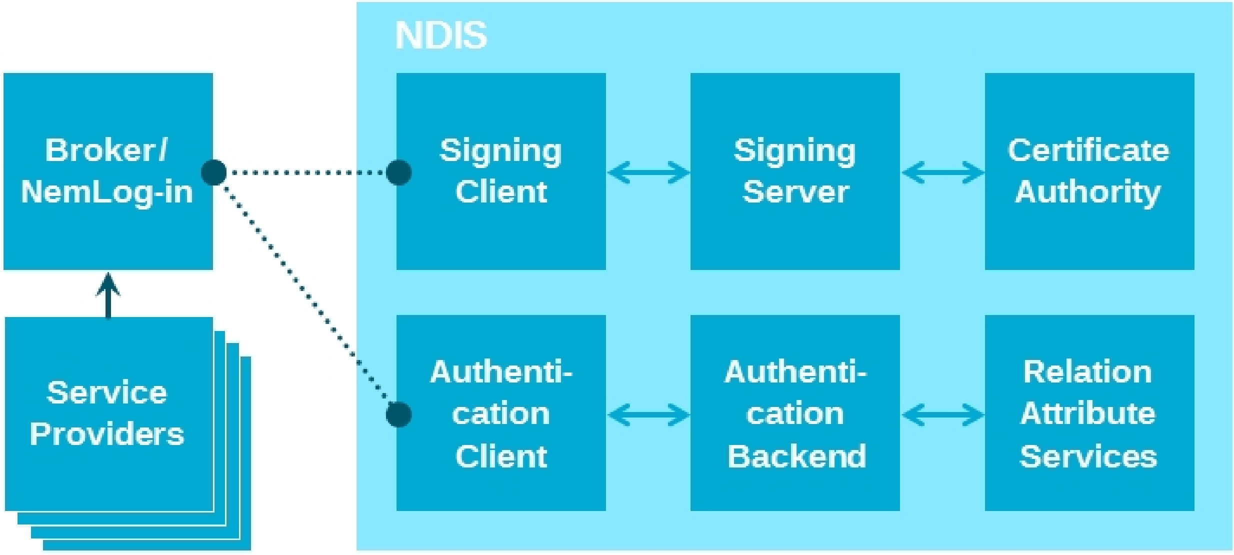
As people move toward using smartphone and tablet apps for the majority of their online interactions, there is a clear benefit to providing more options than a web-based authentication and signing client. What the best solutions are to these challenges, we leave open at this stage.

Parts of the Solution

On the inside, it is expected that the NDIS/ the future solution will consist of the following major areas of functionality:

1. **Identity and Authentication**. Managing the lifecycle of identities and their related credentials
2. **Advanced Electronic Signature**. Securely handling the electronic signing of documents.
3. **Client functionality**. The user-facing parts of the log-in and signing processes.
4. **Business-related functionality**. Functionality aimed specifically at businesses' needs and the need for associating employee IDs with organisations.
5. **Certificate Authority functionality**. The Public Key Infrastructure part of the solution.
6. **System integration functionality**. Adapting the other functionality areas to the existing systems landscape

Along with the functionality areas described above, the solution will integrate closely with its sister platform, "NemLog-in", which is a separate project outside the core NDIS project. NemLog-in serves the role as login broker system for the public sector – the public-facing login solution built on top of the NDIS project described here. It is used by all public sector services, and along with a unified login experience for end users it provides SSO functionality and authorisation functionality to public service providers, as well as related add-on services. A call for tender for the next version of this platform is expected to be issued in parallel with the call for tender for the NDIS solution. As it plays a central role in the structure of the overall solution, it is included in the architectural diagram below.



Exemplified high-level architecture model of the NDIS solution and its relation to NemLog-in, the shared public sector login broker platform.

Identity and Authentication

In the current solution, ID and signature are included in the same solution – the two are based on the same Public Key Infrastructure. Because they are essentially one thing, every login needs to meet the security standards needed for signing, requiring two-factor authentication on every login. There are, however, use-cases that would benefit from easier-to-use less secure single-factor authentication, so to accommodate this the next version of NemID will separate authentication and signing into separate modules that will share credentials whenever higher security is needed. This separation is in line with the eIDAS[1] regulation.

Advanced Electronic Signature

Separating authentication from signing also makes it possible to base the signature module on single-use certificates, where a new signature certificate can be generated for an authenticated user for each new document to be signed. The private key can then be destroyed immediately after signing, obviating the need for securely managing the private keys and thus making tampering even harder. Regardless of the particular technological path taken, any signing solution must live up to the eIDAS requirements for a "qualified" or "advanced" signature as well as the CEN-standard EN 419241[2].

[1] http://tinyurl.com/eidasregulation
[2] http://tinyurl.com/en419241

Client Functionality

Today the main public-facing pieces of the NDIS system are the web-based authentication and signing clients. These will naturally be part of any future solution. But as mentioned above, in the world of mobile platforms this is not always the best solution. Some form of closer integration with existing mobile platforms is likely needed. Whether this be done in the form of dedicated mobile apps, frameworks or tool boxes is still an open question.

Business-Related Functionality

The business-specific functionality focuses on the unique workflows of organisations needing to issue employee IDs that can act on behalf of the organisation. For this, system is needed for both managing identities and handling access rights for those identities – of which there are 1.1 million currently. This area needs some special attention as the current solution is complex due to many different user scenarios and procedures. These IDs will likely continue to be PKI-based in the future as certain business sectors make heavy use of key-on-hardware credentials, local signing servers and other localised solutions that facilitate offline authentication with respect to the central NDIS system – and make high-volume authentication practically feasible.

Certificate Authority Functionality

The Certificate Authority is the Public Key Infrastructure hub that binds the entire public sector infrastructure together. It will be responsible for handling the certificates for system-to-system communication, secure signing, and the certificate-based employee IDs.

System Integration Functionality

The systems landscape surrounding the ID and signing platform is vast and growing so any solution must take into account the ease with which integration can be done. This is key - not only because it is cost prohibitive to change all of the other systems in the landscape - but also because even small disruptions in the user journey through the system will cause confusion.

digst.dk