# Introduction to NemID and the NemID Service Provider Package

# Table of Contents

# Version History

| | | |
|---|---|---|
| 25 February 2014 | Version 2.5 | PHJER |
| 11 April 2014 | Version 2.6 | BMATZ |
| 2 June 2014 | Version 2.7 | PHJER |
| 4 June 2014 | Version 2.8 | PHJER |
| 17 March 2016 | Version 2.9 | KMAIB |
| 5 September 2016 | Version 2.10 | KMAIB |
| 13 September 2016 | Version 2.11 | KMAIB |
| 30 April 2018 | Version 2.12 | RMELG |

## 1 The Purpose and Target Group of the Document

This document is part of the NemID Service Provider Package.

The purpose of this document is to provide a general introduction to NemID and the NemID Service Provider Package, in order to give an overview of the opportunities available and the scope of the implementation.

The document is aimed towards employees at the NemID Service Provider who are responsible for the high level decisions regarding the implementation of NemID.

# 2 Introduction to NemID

NemID is Denmark's security solution for log-in and signing on the Internet.

Please see to the document Terms and concepts in NemID for an explanation of the terms and concepts used in this document and in the NemID Service Provider Package in general (nets.eu/sp-package).

A typical use of NemID is that an end user wishes to log on to a service provider. This is done by the user opening the web page of the service provider and choosing a "Log on" functionality. The service provider will thereby initiate that the end user is authenticated. The result of the authentication is then communicated to the service provider, and based on the result of the authentication the service provider can either choose to reject the end user or to present the end user with a personalised home page.

Please note that the Danish Agency for Digitisation has developed a special service provider package, called "LSS for NemID TU-package" that provides support for tablets and smartphones for users with NemID Employee Certificate with code file in companies using a local signature server (LSS).

This function is now fully integrated in the NemID CodeFile client (Client without OTP) and do not require previously separate implementation by the NemID Service Provider.

The documentation of LSS for NemID is available at https://www.lss-for-nemid.dk.

## 2.1 *Use and Storage of Private Keys*

When a user uses NemID to log on to services or to sign documents on the Internet, seen from a security perspective what happens is that the user uses his or her "private key". The user's private key can be stored in two different ways:

- Central storage: The user's private key is stored on Nets DanID's server. The solution is normally referred to as NemID with code card.

- Local storage: The user stores his or her own private key, either on dedicated USB hardware or in a file on the user's computer. The solutions are normally referred to as NemID Employee Certificate with code file and NemID with hardware.

## *2.2 NemID Clients*

In both scenarios the private key is accessed via a NemID client, which is a utility provided by Nets DanID and run on the user's device (pc or mobile devices).

The NemID clients that the users use to access their private keys are called "Client with OTP" for centrally stored private keys (ref. in technical documentation: NemID JavaScript client) and "Client without OTP" for the locally stored private keys (ref. in technical documentation: NemID CodeFile client).

For a user to access a centrally stored private key, he or she must supply three types of information: A user ID, a password and a one-time password (ref. OTP).

> In online banking solutions it is also possible to log on with only user ID and password, i.e. read-only access to information (Danish: "Konto-kik").

## *2.3 One-Time Passwords*

Users can get one-time passwords from a printed paper card (called a code card), from an electronic device, or via a phone call from Nets DanID (Interactive Voice Response = IVR solution). Or indirectly as a confirmation via a code app.

So there are a number of ways to get one-time passwords. In this document the code card is used as an example.

## *2.4 Where Can NemID be Used?*

Users can use NemID on both pc and mobile devices to log-in and sign documents in online banking solutions, public services such as skat.dk and sundhed.dk, as well as private service providers. On mobile devices, the both centrally stored private keys are supported as well locally stored keys, if the business uses the LSS solution.

In addition, the user may install an extension package, so that NemID can be used for i.e. secure e-mail (in Danish: sikker e-mail). For users with centrally stored keys, there must be installed an extension software, which can be downloaded from www.nemid.nu.

## *2.5 Ordering and Self-Service*

NemID is available for both individuals ("NemID for Citizens") and professionals ("NemID for Business").

NemID for Citizens can be ordered in the user's bank (typically in connection with an agreement of an online banking solution), or in a Citizen Service Centre (in Danish: borgerservice). Users can order NemID at www.nemid.nu, where the user as well finds NemID Self-Service.

NemID for Citizens supports centrally stored private keys as well as private keys stored in hardware tokens.

When ordering NemID a code card is send by letter. Additionally the activation password is send by letter or by SMS. The code card and/or activation password can be handed out at a bank or Citizen Service Centre.

The user can revoke and order extra code cards in NemID Self-Service at www.nemid.nu. Most places that issue NemID can also help the user to revoke NemID and hand out extra code cards.

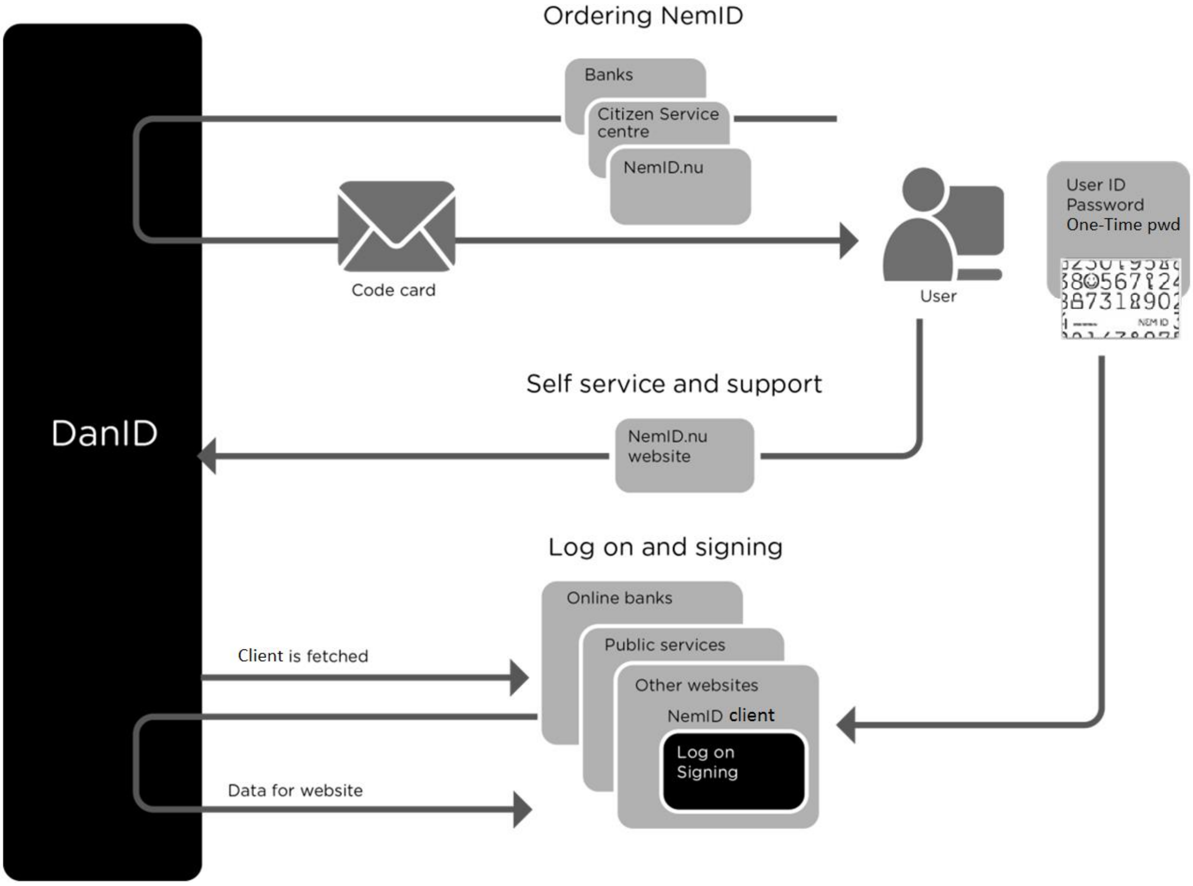


*Figure 1: Subset of an end user's options using NemID*

NemID for Business is available in variations for use by employees and for the IT systems of such businesses. The solution for employees is also known as "NemID Employee Certificates" (Danish: "NemID medarbejdersignatur"). Ordering of NemID Employee Certificates and self-service take place at www.medarbejdersignatur.dk.

NemID for Business supports centrally stored private keys and private keys stored in hardware or key files.

## *2.6 Certificates*

For each private key held by a user, there is a corresponding public key. The public key is used to validate the use of the corresponding private key. For instance, a user may sign a document with his or her private key, after which the public key can be used to validate that the signature is correct. Public keys are therefore made generally available in the form of "certificates". A certificate is a combination of a public key and identity information about the owner of the corresponding private key.

For use by public service providers, a standard for certificates called Public Certificates for Electronic Service (In Danish: Offentlige Certifikater til Elektroniske Service = OCES) has been established. OCES is available in different versions for use by individuals and businesses:

- OCES for individuals is called "POCES"

- OCES for employees is called "MOCES"

- OCES for businesses is called "VOCES"

- OCES for IT systems is called "FOCES"

Banks use their own standard for certificates, while other service providers accept certificates adhering to one or more of the OCES standards.

The

# 3 About the NemID Service Provider Package

NemID Service Provider Package contains the necessary documentation and codes in order for the service provider to test and implement NemID on their site.

The NemID Service Provider can get an overview of, and guidelines on, the processes that the service provider has to complete in order to implement NemID for Citizens and NemID for Business.

## *3.1 Use of the OOAPI*

When choosing a method of implementation for NemID, it is advisable to use Nets DanID’s OOAPI, which is part of the NemID Service Provider Package.

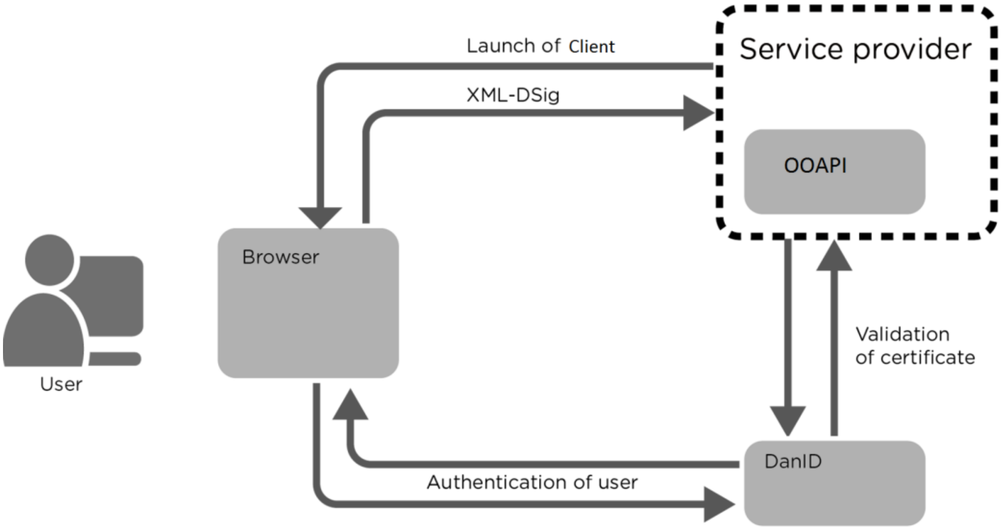


*Figure 2: The role of the OOAPI*

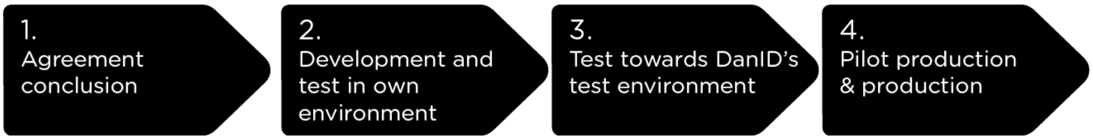
As shown in the figure above, the following takes place when the end user wants to log on to the service provider's site:

1. The end user contacts the service provider.
2. The service provider initiates the launch of one of the NemID clients.
3. The end user is authenticated by Nets DanID via the client.
4. A response is sent to the service provider.
5. The service provider validates the certificate.
6. The user is now authenticated.

If a service provider wishes to transfer its current, customised solution or to use functions not covered by the OOAPI, please see the documents in the NemID Service Provider Package under Reference Documentation for information about direct integration towards the infrastructure.

### 3.2 *The Four Phases of Implementation*

Implementation of NemID involves the following four phases:



1. Agreement conclusion

2. Development and test in own environment

3. Test towards DanID's test environment

4. Pilot production & production

Guide: Order NemID Service Provider

### 3.3 *Entering the NemID Service Provider Agreement*

To become a NemID Service Provider, a NemID Service Provider Agreement must be entered with Nets DanID, defining the current terms and conditions for service providers.

The NemID Service Provider Package withholds two documents: Standard terms and conditions for receiving OCES certificates from Nets DanID and General Terms and Conditions.

### 3.4 *Special Conditions for Public Service Providers*

Public service providers that are considering using NemID have two options in regards to integration:

- Integration via NemLog-in or Virk.dk. Please find the integration guidelines for NemLog-in at www.skat.dk and for virk.dk at www.virk.dk

- Integration directly via their own solutions.

In both scenarios the public service provider is to enter the NemID Service Provider Agreement with Nets DanID.

# 4 Implementation at the Service Provider

When a NemID Service Provider Agreement has been entered with Nets DanID, the service provider can start to implement the solution on the website and in mobile applications.

Guide: test og implementering, nets.eu/tu-guide (In Danish).

## 4.1 *Authentication and Signing Options*

As mentioned in the introduction, there are two ways in which a user’s private key can be stored: centrally or locally. Service providers should therefore present the users with the two different clients in order to support both options. The two clients are called the NemID JavaScript client and the NemID CodeFile client.

### *4.1.1 The NemID JavaScript Client (Client with OTP)*

“Client with OTP”, being the so called the NemID JavaScript client is used where the user’s private key is stored on a central server at Nets DanID.

Scenarios in the following solutions:

- NemID with code card – where the user gets one-time passwords from a code card or from a large-letter code sheet.
- NemID with code token – where the user gets one-time passwords from an electronic device.
- NemID with IVR – where the user gets one-time passwords via a phone call from Nets DanID.
- NemID with code app – where the user confirms the transaction via a code app installed on a mobile device.

In general the solution NemID with code card, is where the client calls the private key server at Nets DanID in order to perform authentication and signing. Such solutions are useable by both NemID for Citizens and NemID for Business.

The NemID JavaScript client is supported in most browsers and does not require plugins on the end user’s platform. Therefore, the client can be used on most mobile devices.

### *4.1.2 Client without OTP*

“Client without OTP”, being the so called the NemID CodeFile client is used whenever the user’s private key is stored locally.

This is the case for the following solutions:

- NemID Employee Certificate with key file – where the user’s private key belonging to MOCES, VOCES, or FOCES certificates is kept in a file on the user’s pc.

- NemID on hardware – where the user’s private key belonging to POCES and MOCES certificates is kept on a hardware token in the user’s possession.

The NemID CodeFile client is supported in most browsers  the support the required Java plugins (Java or NemID code file software) that is to be installed on the users’ pc for the user to be able to access the locally stored private key. Therefore this solution cannot be utilised on mobile devices.

In businesses using LSS the user with NemID Employee Certificate with code file will be able to use the NemID CodeFile client in most browsers, both from the pc and mobile devices.

### *4.1.3 Activation of Clients*

The user must on the service providers site choose login method.

The service provider should show the relevant options for the user and assure that the correct client is loaded i.e. Log on with NemID code card.

In the visual guidelines the service provider can find recommendations and guidance on how to integrate of NemID.

> In the NemID Service Provider Package you find UX guidelines, Løsningsbeskrivelse og visuelle guidelines (in Danish).

## *4.2 Scope of Implementation*

Nets DanID estimates that it will take a service provider between one and four weeks to implement NemID.

The estimated time spend depends on the existing solution and only covers the technical implementation process.

# 5 Launching the Client

As described in section 4 **Implementation at the Service Provider**, the service provider must provide the user with a choice between two login methods. The service provider must then load either the JavaScript client or the NemID CodeFile client.

Is both scenarios the client is located on a server at Nets DanID and must be transferred from this server.

## *5.1 Launch/Setup of the NemID JavaScript Client*

In order to load the NemID JavaScript client, the service provider must open a web page with an iframe pointing to a specific URL at Nets DanID's server.

A set of parameters are sent to the iframe in order to control the user interface of the client. Along with the parameters, a hash value (SHA-256) of the parameters on normalised form plus a signature of the hash value, created with the private key belonging to the service provider's VOCES or FOCES certificate, is sent to the client.

The NemID Service Provider Package includes the following elements that can help the service provider in setting up the solution:

- Java and .Net reference code for the generation and signing of the hash value of the normalised client parameters.
- Examples of how this Java and .Net code can be included on a service provider's website.
- Description of the Java and .Net code.

## *5.2 Launch/Setup of the NemID CodeFile client*

The launch of the NemID CodeFile client is similar to the launch of the NemID JavaScript client (see Paragraph 5.1).

## *5.3 Visual Implementation (Setup)*

Nets DanID has developed a set of graphical designs which, among other things, recommends how to present the two clients to the users.

### *5.4 Client Interaction with Nets DanID*

After the “Client with OTP” has been loaded, an authentication process is conducted through it. In connection with this, the client communicates with Nets DanID’s infrastructure.

When the user authentication process has been successfully completed, the client sends an XML-DSig response to the service provider’s web server containing the user’s signature and certificate.

The service provider must then validate the user’s signature and certificate. See Paragraph 6 **Validation of Certificate**.

# 6 Validation of Certificate

Regardless of whether the user has chosen NemID with code card, NemID Employee Certificate with code file or NemID with hardware, the task of validating the certificate is the same.

There are essentially two ways to perform the validation. The service provider either use the OOAPI from Nets DanID or develop your own validation module and access the components in the infrastructure such as certificate revocation lists (CRLs) and PID/RID services directly.

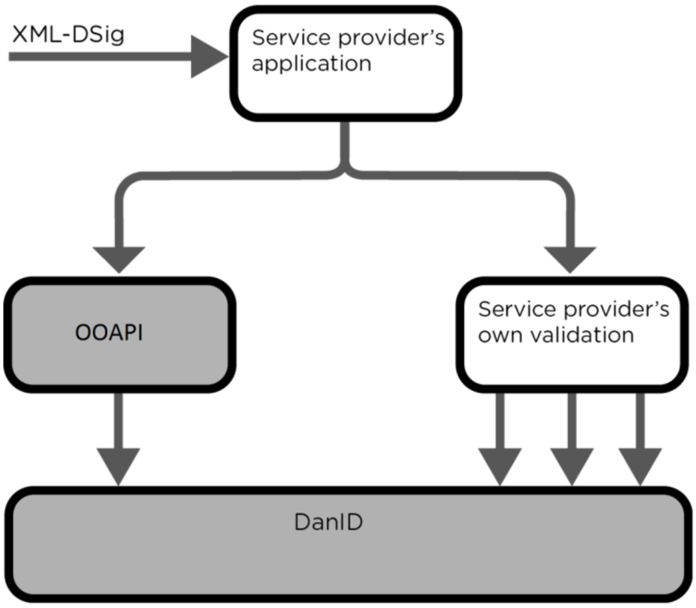

XML-DSig
Service provider's application
OOAPI
Service provider's own validation
DanID

*Figure 3: Validation of certificate*

## *6.1 OOAPI from Nets DanID*

If the service provider chooses to use the OOAPI from Nets DanID, the service provider must call a function that withholds the response from the authentication. The function responds with a PID/RID number if the certificate is valid. If the certificate is invalid, an error code is returned.

A full Java and .Net documentation for the OOAPI is made available, together with complete reference code in Java and .Net.

👁 Find more information in the specification documents for PID/RID services in the NemID Service Provider Package.

## 6.2 *Direct Infrastructure*

For service providers that do not wish to use Nets DanID’s OOAPI, there is the option of developing their own dedicated solution and accessing the individual components in the infrastructure directly.

The NemID Service Provider Package contains specifications for how each of the following components in the infrastructure can be accessed directly:

1. PID service
2. RID service
3. OCSP responder
4. Full certificate revocation list accessible via LDAP
5. Full certificate revocation list accessible via HTTPS
6. Partial certificate revocation lists accessible via LDAP

> Please see Tools and Specification documentation in the NemID Service Provider Package.

# 7 Test Environment

Nets DanID has an environment available to service providers for development and testing.

Furthermore, Nets DanID has developed a set of tools (”Developer Site”), which can be used to test and verify input parameters and signatures for use with the NemID JavaScript client.

Access to the test environment and the Developer Site is provided when entering the NemID Service Provider Agreement.

> To access Developer Site and test environment the service provider’s IP addresses must be whitelisted at two different sites: Developer Site and Pre Production (PP).

## 8 Support

Help and guidance for the entire process is available at nets.dk under Support (in Danish: Kundeservice) for NemID Service Providers (in Danish NemID tjenesteudbyder).

Nets DanID can help with implementation, development and integration of NemID in your solution.

To contact The Service Provider Support use the web formula at nets.dk, nets.eu/tu-en-support.

Modifications and necessary adaptations in the service provider's own environment must be performed by the service provider's own resources.

Nets DanID offers two service packages; one for integration of NemID in your solution and another for ongoing maintenance and support of your NemID solution. Please find more information on nets.eu/nemid-servicepackages