Nets DanID A/S
Lautrupbjerg 10
DK – 2750 Ballerup

T +45 87 42 45 00
F +45 70 20 66 29
info@danid.dk
www.nets-danid.dk

CVR no. 30808460

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

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 create the necessary overview of the opportunities available and the scope of the implementation.

The document is aimed at the people at the 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 logging on and signing on the Internet.

> Please refer to the document entitled **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.

A typical use of NemID is that an end user wishes to log on to a service provider. This is accomplished 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 in companies using a local signature server (LSS).
>
> Service providers, who plan to support NemID employee signature with OTP key card on mobile devices, should also support NemID employee signature on local signature server. NemID documentation from Nets DanID does NOT include the LSS for NemID solution. 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, what happens from a security perspective 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
- Local storage: The user stores his or her own private key, either on a piece of dedicated hardware or in a file on the user's computer.

2.2 NemID Clients

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

The NemID clients that the users use to access their private keys are named "Client with OTP" (for centrally stored private keys) and "Client without OTP" (the locally stored private keys).

For a user to access a centrally stored private key, he or she must supply three pieces of information: a user ID, a password and a one-time password.

> In certain online banking solutions it is also possible to log on solely by supplying the user ID and password, for example for read-only access to account 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 (the IVR solution - "Interactive Voice Response").

So there are a number of ways to get one-time passwords. The remainder of this document uses the code card as an example.

2.4 Where Can NemID be Used?

Users can use NemID on both PCs and mobile devices to log on to and to sign documents in online banking solutions, public services such as skat.dk and sundhed.dk, as well as private service providers. On mobile devices, only centrally stored private keys are supported.

In addition, the user may install an extension pack, so that NemID can be used for secure e-mail, for example. The software for this 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 a variety of locations, e.g. the user's bank (typically in connection with the conclusion of an online banking solution agreement), or from a Citizen Service Centre (Danish: "Borgerservicecenter"). Furthermore, individuals can order NemID on their own at www.nemid.nu, which is also the place for users' self-service.

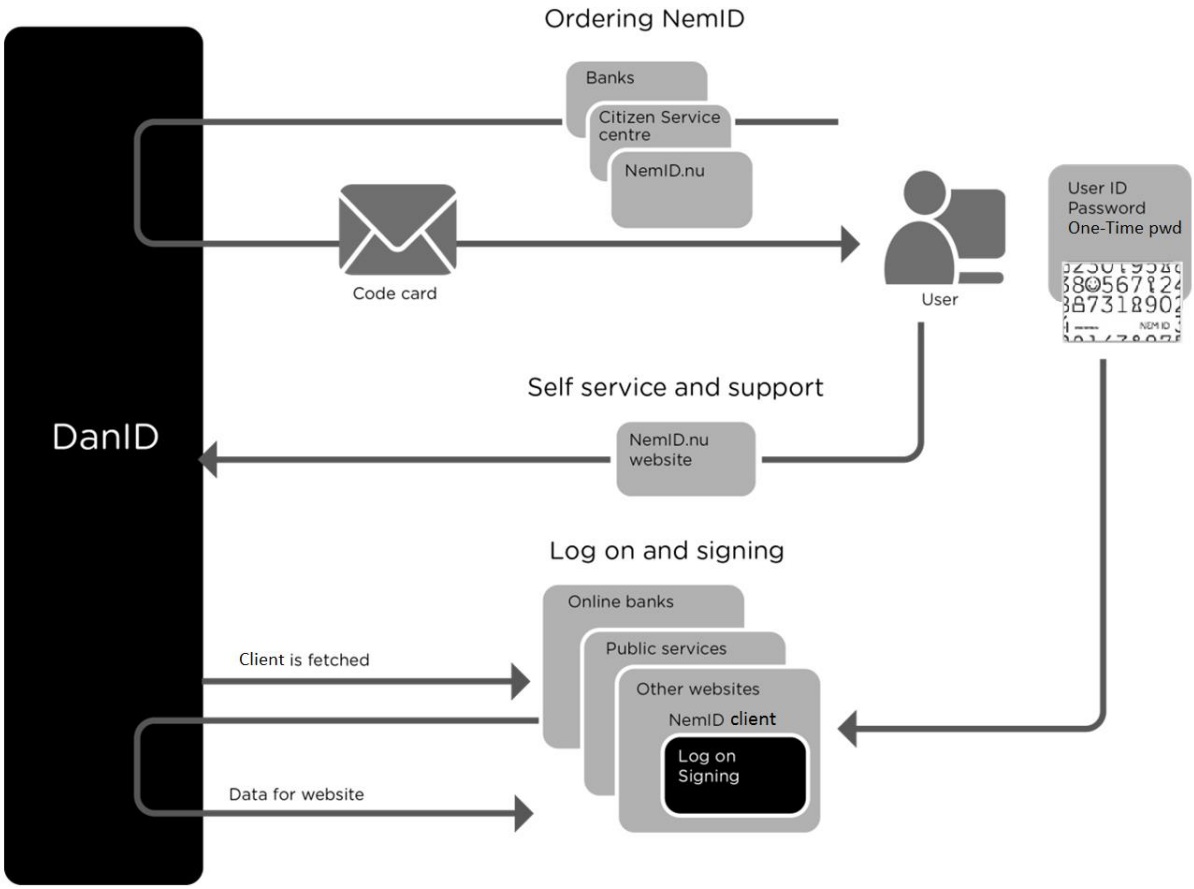


Figure 1: Subset of an end user's options using NemID

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

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

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

For centrally stored private keys, the code cards are sent through the post. In addition, the activation password may be sent through the post or by SMS. Furthermore, for NemID for Citizens, the code card and/or activation password may under certain circumstances be handed out at a bank or citizen service centre.

Most places that issue NemID can also help the user with revocation of certificates or supplying extra code cards. The user can also use NemID's self-service portal, www.nemid.nu, for such purposes, or contact NemID support.

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 OCES - "Offentlige Certifikater til Elektroniske Service" (English: "Public Certificates for Electronic Service") 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.

Note that, in everyday language, certificates are sometimes referred to as if they were synonymous with their corresponding private key. Thus, one may be encouraged to "sign a document using a VOCES", although it is technically the private key belonging to the certificate rather than the certificate itself that is used for signing.

3 About the NemID Service Provider Package

The NemID Service Provider Package is a collection of documents and software that provides new and existing service providers with an overview of, and guidelines on, the processes that the individual service provider has to complete in order to implement NemID for Citizens and Business.

The NemID Service Provider Package is designed to take into account the different implementation needs that might exist with different kinds of service providers.

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.

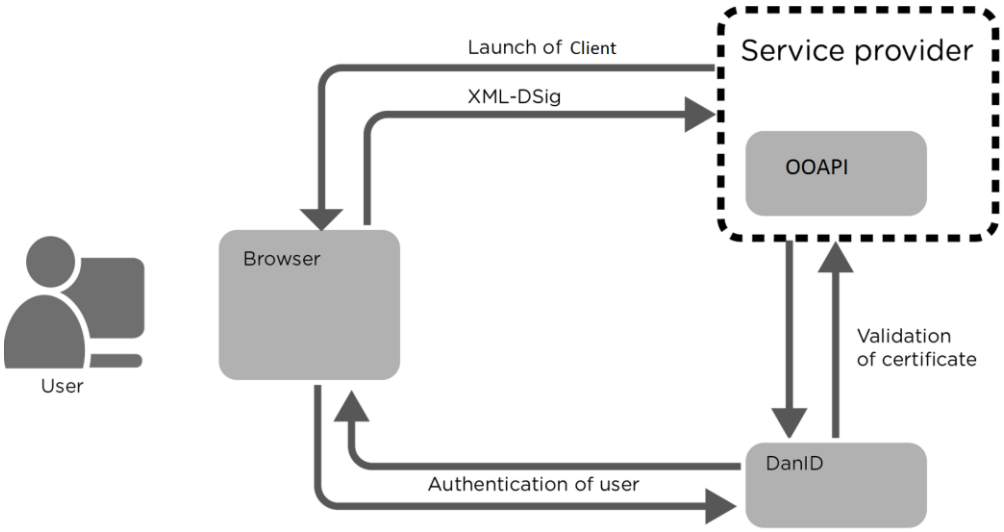


Figure 2: The role of the OOAPI

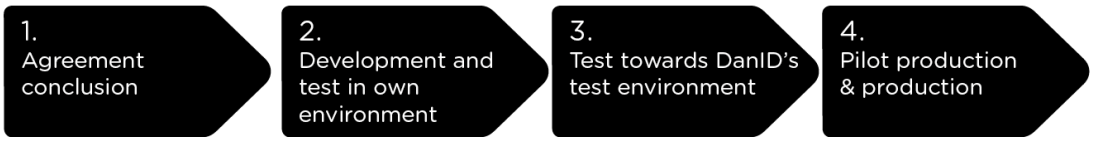
As shown in the figure above, the following takes place when the end user wants to log on to the service provider's site:

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 refer to the documents under **Reference Documentation** in section 1 for information about direct integration to the infrastructure.

3.2 The Four Phases of Implementation

Implementation of NemID involves the following four phases:



At www.nets-danid.dk/tu we have created a step-by-step guide which takes you through all the steps from signing the agreement, test, and implementation to release.

3.3 Concluding the Service Provider Agreement

To become a service provider, a Service Provider Agreement must be concluded with Nets DanID, describing the current terms and conditions for service providers.

Terms and conditions for the Service Provider Agreement can be found at www.nets.eu/dk-da/Produkter/Sikkerhed/NemID-tjenesteudbyder/Pages/Vilk%C3%A5r.aspx

3.4 Special Conditions for Public Service Providers

Public service providers that are considering using NemID have two connection options:

- Integration via NemLog-in or Virk.dk. Please refer to the integration guidelines for NemLog-in at www.skat.dk/nemlog-in and for virk.dk at www.virk.dk

- Integration directly via their own solutions.

4 Implementation at the Service Provider

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

The Service Provider Agreement can be obtained by contacting Nets DanID Sales at salg@danid.dk or by downloading it at www.nets-danid.dk/tu.

4.1 Authentication and Signing Options

As mentioned in the introduction, there are two different ways in which a user's private key can be stored: centrally or locally. Service providers should therefore, as a general rule, present the users with two different clients in order to support both methods. As mentioned earlier, the two clients are called "Client with OTP" and "Client without OTP" respectively.

4.1.1 Client with OTP

"Client with OTP" is used in cases where the user's private key is stored on a central server at Nets DanID.

This is the case 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 telephone call from Nets DanID.

Generally speaking, "Client with OTP" handles solutions where the client contacts 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 employee certificates.

"Client with OTP" works in modern browsers and does not require plugins on the end user's platform. Therefore, the client can be used on most mobile units (as opposed to "Client without OTP").

4.1.2 Client without OTP

"Client without OTP" (also known as the "OpenSign applet") is used whenever the user's private key is stored locally.

This is the case for the following solutions:

- 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.

- NemID in key file – where the user's private key belonging to MOCES, VOCES, or FOCES certificates is kept in a file on the user's computer.

"Client without OTP" requires that Java is available in the end user's browser, and will therefore not be available on mobile units.

4.1.3 Activation of Clients

The user must choose on the website which of the two login mechanisms ("Client with OTP" or "Client without OTP") is to be used. On its website, the service provider must display the relevant options for the user and make sure that the correct client is launched. For this purpose, Nets DanID has developed a set of visual guidelines, which are part of the NemID Service Provider Package.

In the document entitled **Visual Guidelines**, service providers can read more about how this option can be presented and which elements should be used to give the user the best possible guidance.

For a more detailed description of how to interface with the two clients, please refer to section 5 **Launching the Client** and section 6 **Validation of Certificate**.

Please also refer to the documents in the folder entitled **Implementation Documentation**.

4.2 Scope of Implementation

Nets DanID estimates that it will take a service provider between 1 and 4 weeks to implement NemID.

The estimated resource consumption depends on the existing solution and only covers the technical implementation process, i.e. excluding the initial agreement discussions, testing, etc.

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 launch either "Client with OTP" or "Client without OTP".

The "Client with OTP" is located on a server at Nets DanID and must be transferred from this server.

The "Client without OTP" is also located on a server at Nets DanID, and should be transferred from there. It is also possible to have this client stored locally at the service provider, and in such cases it is the responsibility of the service provider to synchronize its local copy with the official client.

Read more about setting up the two clients in the document entitled **NemID Implementation Guidelines** under **Documentation**.

5.1 Launch/Setup of "Client with OTP"

In order to launch "Client with OTP", 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 "Client without OTP"

The current "Client without OTP" is described in detail at OpenOCES.org, where all relevant implementation documentation can be found.

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.

For a more detailed description of this recommendation, please refer to the document entitled **Visual Guidelines** under the heading **Documentation**

5.4 Client Interaction with DanID

After the "Client with OTP" has been launched, 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 section 6 **Validation of Certificate**.

6 Validation of Certificate

Regardless of whether the user has chosen to use the client with or without OTP, the task of validating the certificate is the same. There are essentially two different ways of performing this validation. You can either use the OOAPI from Nets DanID or develop your own validation module and access the infrastructure components such as certificate revocation lists (CRLs) and PID/RID services directly.

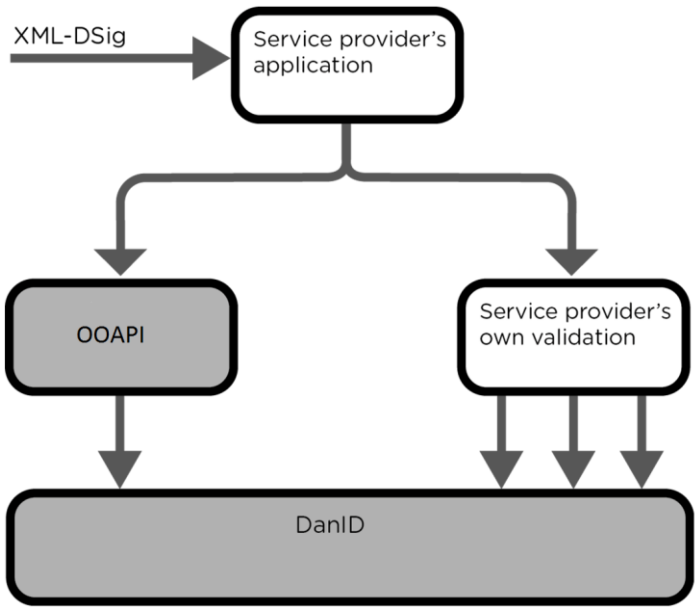


Figure 3: Validation of certificate

6.1 OOAPI from Nets DanID

If a service provider chooses to use the OOAPI from Nets DanID, the service provider must call a function with the response from the authentication. The function responds with a PID/RID number if the certificate is valid (see specification documents for PID-CPR and RID-CPR services as mentioned in section 1 for details regarding these numbers). If the certificate is invalid, an error code is returned.

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

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 infrastructure components directly.

The NemID Service Provider Package contains specifications for how each of the following infrastructure components 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 refer to the documents in the folder entitled **Tools and reference documentation**, which is part of the NemID Service Provider Package.

Please also consult section 3.1 **Use of the** OOAPI.

7 Test Environment

Nets DanID makes an environment available to all current and future service providers for development and testing.

Furthermore, Nets DanID has developed a set of tools (”Developer Tools”), which can be used to test and verify input parameters and signatures for use with “Client with OTP”. Access to the test environment and the developer tools is provided after conclusion of the Service Provider Agreement.

Please refer to the guide at www.nets.eu/dk-da/Produkter/Sikkerhed/NemID-tjenesteudbyder/Pages/default.aspx#tab3

8 Support

Service providers can find help and guidance for the entire process at http://www.nets.eu/dk-da/Service/kundeservice/nemid-tu/Pages/Skriv-til-NemID-tjenesteudbyder-support.aspx.

Nets DanID also offers support to service providers in the following areas:

- Information about Nets DanID documentation
- Information about the use of security modules and interfaces
- Information about the use of the necessary certificates.

Support is available by contacting tu-support@danid.dk and is provided at the current hourly rate.

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