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

Recommended test procedures

Table of Contents

Version history

24 February 2010	Version 1.0	MOBO
22 March 2010	Version 1.1	MTV
10 June 2010	Version 1.2	MTV
23 January 2011	Version 1.3	MTV
17 October 2012	Version 1.4	MTVOL
19 March 2014	Version 1.5	BMATZ
2 June 2014	Version 1.6	PHJER
25 September	Version 1.7	STNOR

1. Purpose and target group

This document is a part of the NemID Service Provider Package.

The purpose of the document is to provide guidance on how the service provider can test whether the implementation is working correctly.

The document is aimed at the person responsible for planning and conducting tests at the service provider.

2. Tests

This test document describes Nets DanID's recommendations of the tests that the service provider should conduct before integration takes place with Nets DanID's production system.

The document starts by describing a number of functional areas that should be tested before the actual tests on use cases commence.

In the event of any errors, these can be reported to Nets DanID at:

http://www.nets.eu/dk-da/Service/kundeservice/nemid-tu/Pages/Skriv-til-NemID-tjenesteudbyder-support.aspx

3. Functional tests

Before the use case-based test procedure commences, you should make sure that the most basic elements of the system have been thoroughly tested.

Below are the most important areas for this kind of test.

3.1 Generation and signing of applet parameters

If the applet is not set up correctly, it closes down and returns an error code to the service provider. A list of error codes can be found in the service provider package in folder 2 – Implementation documentation.

If the applet is set up correctly, it contacts Nets DanID's server and validates that the startup parameters are correctly signed with a valid VOCES certificate and that Nets DanID has an agreement with the accompanying service provider ID. If this is not the case, the applet returns error code SRV001 to the service provider.

If the applet starts up and displays its startup screen with a logon, the applet is set up correctly. All the service provider needs to check is that its name is displayed correctly in the applet.

3.2 Receive and validate XMLSig response from the applet

The service provider's system must be able to receive the XMLDSig that is sent to the web server via the live connect call backs used by the applet.

The XMLDSig response must then be validated to check whether it has been correctly signed.

3.3 Validate certificate

To validate the certificate, the following steps must be followed:

1. Extract the certificate from XMLDSig
2. Validate the certificate and identify CA as OCES I or OCES II throughout the whole certificate chain to the root certificate
3. Check that the certificate has not expired
4. Check that the certificate is not revoked

If the service provider is using the security package from Nets DanID, it is sufficient to validate whether the method in OOAPI returns a correct response.

3.4 PID

The service provider must be able to extract the PID from the certificate.

If the service provider uses a CPR no. to identify the user, the PID service must be used. Depending on the application method, the service provider must either translate PID into CPR no. or also create a matched lookup to determine whether the CPR no. provided by the user matches the PID number.

Both tests require the service provider to have concluded a specific agreement with Nets DanID on the use of the PID service.

3.5 RID

The RID service is used if MOCES employee certificates with assoiciated CPR numbers need to be validated.

4. NemID for Citizens – Logon test cases

The following section describes the most important test cases that you must conduct in order to make sure that your system is able to use NemID for citizens (Private) and to handle the most common citizen situations.

4.1 User with NemID logs on for the first time

This is a positive test that is completed successfully when the user has logged on to the service provider's self-service universe using NemID with a code card or code token.

1. The user enters the service provider's website in order to log on to its self-service universe.
2. The user locates the logon button or a corresponding link, and clicks on it.
3. The page then changes to the logon web page with NemID and Digital Signature.
4. This is the first time that the user has entered the web page and therefore has no cookie stored.
5. The system places a cookie on the user's computer.
6. The user enters his/her user ID.
7. The user enters his/her PIN code.
8. The system prompts the user for a four-digit code number (#) from the user's code card.
9. The user enters his/her six-digit code from the code card.
10. The web page changes to the service provider's self-service universe, where the user is identified.

4.2 User with NemID for bank only logs on

This is a negative test that is completed successfully when the user with a NemID with a code card/code token has been prevented from logging on to the service provider's self-service universe.

The user for this test should be a private user, older than 15 years and not qualified to use POCES.

1. The user enters the service provider's website in order to log on to its self-service universe.

2. The user locates the logon button or a corresponding link, and clicks on it.

3. The web page changes and the NemID logon screen appears.

4. The user enters his/her user ID.

5. The user enters his/her password.

6. The system returns an error code to the service provider. The error code will dependent on the identity type, see the list of error codes in the service provider package in folder 2 – Implementation documentation.

7. The service provider displays an error text.

4.3 User with blocked (time locked) NemID logs on

This is a negative test that is completed successfully when the user with a NemID with a code card/code token has been prevented from logging on to the service provider's self-service universe and has received an error message in the applet.

1. The user enters the service provider's website in order to log on to its self-service universe.
2. The user locates the logon button or a corresponding link, and clicks on it.
3. The web page changes and the NemID logon screen appears.
4. The user enters his/her user ID.
5. The user enters his/her password.
6. The system displays an error text in the applet to the effect that the user cannot log on until the time lock has been removed.
7. The system returns error code AUTH004 to the service provider.
8. The service provider can display a text to the user in connection with error code AUTH004.

4.4 User with locked (permanent) NemID logs on

This is a negative test that is completed successfully when the user with a NemID with a code card/code token has been prevented from logging on to the service provider's self-service universe and has received an error message with a link to support at www.nemid.nu.

1. The user enters the service provider's website in order to log on to its self-service universe.
2. The user locates the logon button or a corresponding link, and clicks on it.
3. The web page changes and the NemID logon screen appears.
4. The user enters his/her user ID.
5. The user enters his/her password.
6. The system displays an error text in the applet to the effect that the user cannot log because his/her NemID has been blocked.
7. The system returns error code AUTH005 to the service provider.
8. The service provider displays the error text for error code AUTH005 and the user is referred to support at www.nemid.nu.

5. NemID for Citizens - Signing test cases

The service provider must validate that the signed text is displayed correctly in the applet.

The test cases that are defined in section 4 for logon can also be relevant for signing. The starting point is that the same signature must be used for both logon and signing. In this case this test has already been conducted when testing the logon function.
The situation is, however, that as a service provider you do not necessarily require the user to be logged on before a text is signed. In this situation Nets DanID recommends that you also conduct the test cases that are described under logon.

5.1 User signs text written in plain text with NemID with code card/code token

This is a positive test that is completed successfully when the service provider has validated that the signed text in the response from the applet is identical with the text that was sent for signing.

1. The user enters the service provider's website and selects the function that requires him to sign a text.
2. The service provider sends the desired text to the applet as a parameter.
3. The web page changes and the signing logon screen for signing with NemID is displayed on screen.
4. The user validates that the text is displayed correctly.
5. The user enters his/her user ID.
6. The user enters his/her password.
7. The system prompts the user for a four-digit code number (#) from the user's code card.
8. The user enters his/her six-digit code from the code card.
9. The system returns the signed response text to the service provider.
10. The service provider validates that the response text is identical with the text that was given to the applet in item 2.

5.2 User signs text written in HTML with NemID with code card/code token

This is a positive test that is completed successfully when the service provider has validated that the signed text in the response from the applet is identical with the text that was sent for signing.

1. The user enters the service provider's website and selects the function that requires him to sign a text.
2. The service provider sends the desired text to the applet as a parameter.
3. The web page changes and the signing screen for signing with NemID appears on screen.
4. The user validates that the text is displayed correctly. Here HTML is used, and it is important that the formatting options that the service provider wishes to be used are also displayed as expected.
5. The user enters his/her user ID.
6. The user enters his/her password.
7. The system prompts the user for a four-digit code number (#) from the user's code card.
8. The user enters his/her six-digit code from the code card.
9. The system returns the signed response text to the service provider.
10. The service provider validates that the response text is identical with the text that was given to the applet in item 2.

5.3 User signs text written in XML with NemID with code card/code token

This is a positive test that is completed successfully when the service provider has validated that the signed text in the response from the applet is identical with the text that was sent for signing.

1. The user enters the service provider's website and selects the function that requires him to sign a text.
2. The service provider sends the desired XML text and XML stylesheet to the applet as parameters.
3. The web page changes and the signing screen for signing with NemID is displayed on screen.
4. The user validates that the text is displayed correctly. Here XML is used, and it is important that the formatting options that the service provider wishes to be used are also displayed as expected.
5. The user enters his/her user ID.
6. The user enters his/her password.
7. The system prompts the user for a four-digit code number (#) from the user's code card.
8. The user enters his/her six-digit code from the code card.
9. The system returns the signed response text to the service provider.
10. The service provider validates that the response text is identical with the text that was given to the applet in item 2.
11. The service provider validates that the response also contains information about the style sheet that was used when signing.

5.4 User signs PDF document with NemID with code card/code token

This is a positive test that is completed successfully when the service provider has validated that the signed text in the response from the applet is identical with the text that was sent for signing.

1. The user enters the service provider's website and selects the function that requires him to sign a PDF.
2. The service provider sends the desired PDF to the applet as a parameter.
3. The web page changes and the signing screen for signing with NemID is displayed on screen.
4. The user validates that the document is displayed correctly
5. The user enters his/her user ID.
6. The user enters his/her password.
7. The system prompts the user for a four-digit code number (#) from the user's code card.
8. The user enters his/her six-digit code from the code card.
9. The system returns the signed response text to the service provider.
10. The service provider validates that the response text is identical with the text that was given to the applet in item 2.

6. NemID for Citizens - Other test cases

For NemID for Citizens it is recommend that the service provider tests their implementation by going through the following test cases.

6.1 User with MOCES II and logon to NemID for Citizens

If you as a service provider have decided that you only want login and signing with private identities and not employee identities you should also test that this is set up properly, by trying to log on with an employee signature. The result should be that the employee user is not allowed to log on.

7. NemID for Business – Log-in test cases

For NemID for Business it is recommend that the service provider tests their implementation by going through the following log-in test cases.

7.1 User with NemID (Code card) logs on

Purpose of the test case:

That an employee with a valid NemID for Business employee signature with a code card can log on to the service providers site.

Prerequisites:

A functioning (public) service provider site

A valid NemID for Business employee signature with a code card

Test cycle:

Login

Status after the test:

The employee is logged on at the service provider's site.

7.2 User with NemID (Software certificate) logs on

Purpose of the test case:

That an employee with a valid NemID for Business employee signature as a software certificate can log on to the service providers site.

Prerequisites:

A functioning (public) service provider site

A valid NemID for Business employee signature as a software certificate

Test cycle:

Login

Status after the test:

The employee is logged on at the service provider's site.

7.3 User with a Digital Signature (Employee signature logs on

Purpose of the test case:

That an employee with a valid Digital Signature (employee signature) can log on to the service providers site.

Prerequisites:

A functioning (public) service provider site

A valid Digital Signature (employee signature)

Test cycle:

Login

Status after the test:

The employee is logged on at the service provider's site.

7.4 User with a time-locked NemID (Code card) logs on

Purpose of the test case:

That an employee with a time-locked NemID for Business employee signature with a code card cannot log on to the service providers site.

Prerequisites:

A functioning (public) service provider site

A valid time-locked NemID for Business employee signature with a code card

Test cycle:

Login

Status after the test:

The employee is not logged on at the service provider's site.

7.5 User with a revoked NemID (Code card) logs on

Purpose of the test case:

That an employee with a revoked NemID for Business employee signature with a code card cannot log on to the service providers site.

Prerequisites:

A functioning (public) service provider site

A valid time-locked NemID for Business employee signature with a code card

Test cycle:

Login

Status after the test:

The employee is not logged on at the service provider's site.

7.6 User with a revoked NemID (Software certificate) logs on

Purpose of the test case:

That an employee with a time-locked NemID for Business employee signature as a software certificate cannot log on to the service providers site.

Prerequisites:

A functioning (public) service provider site

A valid time-locked NemID for Business employee signature as a software certificate

Test cycle:

Login

Status after the test:

The employee is not logged on at the service provider's site.

7.7 User with a revoked Digital Signature (Employee signature) logs on

Purpose of the test case:

That an employee with a revoked Digital Signature (Employee signature) cannot log on to the service providers site.

Prerequisites:

A functioning (public) service provider site

A revoked Digital Signature (Employee signature)

Test cycle:

Login

Status after the test:

The employee is not logged on at the service provider's site.

8. NemID for Business – Signing test cases

For NemID for Business it is recommend that the service provider tests their implementation by going through the following signing test cases.

8.1 User with NemID (Code card) signs text

It is recommended to test the signing of text written in:

- Plain text
- HTML
- XML
- PDF

Purpose of the test case:

That an employee with a valid NemID for Business employee signature with a code card can sign plain text, HTML and XML respectively at the service provider's site.

Prerequisites:

A functioning (public) service provider site

A valid NemID for Business employee signature with a code card

Test cycle:

Signing

Status after the test:

The employee can perform signings at the service provider's site.

8.2 User with NemID (Software certificate) signs text

It is recommended to test the signing of text written in:

- Plain text
- HTML
- XML
- PDF

Purpose of the test case:

That an employee with a valid NemID for Business employee signature as a software certificate can sign plain text, HTML and XML respectively at the service provider's site.

Prerequisites:

A functioning (public) service provider site

A valid NemID for Business employee signature as a software certificate

Test cycle:

Signing

Status after the test:

The employee can perform signings at the service provider's site.

8.3 User with a Digital Signature (Employee signature) signs text

It is recommended to test the signing of text written in:

- Plain text
- HTML
- XML
- PDF

Purpose of the test case:

That an employee with a valid Digital Signature (Employee signature) can sign plain text, HTML and XML respectively at the service provider's site.

Prerequisites:

A functioning (public) service provider site

A valid Digital Signature (Employee signature)

Test cycle:

Signing

Status after the test:

The employee can perform signings at the service provider's site.

9. NemID for Business - Other test cases

For NemID for Business it is recommend that the service provider tests their implementation by going through the following test cases.

9.1 User with POCES II and logon to NemID for Business

If you as a service provider have decided that you only want login and signing with employee identities and not private identities you should also test that this is set up properly, by trying to log on with an private/citizen signature. The result should be that the citizen user is not allowed to log on.

10. Multiple Issuing CA – test cases

As multiple Issuing CAs, has been implemented it is relevant to test the certificates issued by each Issuing CA is handled properly. This is done by testing the NemID functionality with certificates issued by each Issuing CA.

10.1 Create test certificates

Since the test certificates in the test environment (PP) by default is issued from the active CA, there is a need to do the following to issue test certificates from the other CAs:

When issuing test certificates, the following can be included as part of the citizen's / employee's certificate name (separated by space).

• If "selectca-ica" is included in the certificate name, these will be issued from the currently active CA.

• If "selectca-ocai" included in the certificate name, these will be issued from the next newest CA.

• If "selectca-ocaii" included in the certificate name, these will be issued from the third newest CA etc.

Note that selectca names should be without "".

By march 2014 two issuing CAs has been implemented. Ica (the new CA) and ocai (the old CA).

10.2 Employee with a valid NemID for Business log on and sign

Test Objective:

- That the employee with a valid NemID Business certificate can log on to service provider's site and sign a document

Prerequisites:

- Service Provider Site that works

To be tested with the following certificates:

- Valid NemID for Business employee signature with Key Card issued by each Issuing CA
- Valid NemID for Business employee signature with Key File issued by each Issuing CA
- Valid NemID for Business employee signature with HW issued by each Issuing CA

Are several types of revocation list used (CRL Full, Partial CRL and OCSP), test is carried out in all used revocation list types.

Test scenario:

- Log on to the service provider's site
- Sign supported types of documents
  - Text
  - XML
  - HTML
  - PDF

Status after the test:

- Employee is logged on service provider's website and sign a document

10.3 Employee with a revoked NemID for Business log on and sign

Test Objective:

- That an employee with a revoked NemID for Business is not able to log on to service provider's site and not able to sign documents

Prerequisites:

- Service Provider Site that works

To be tested with the following certificates:

- Revoked NemID for Business employee signature with Key Card issued by each Issuing CA
- Revoked NemID for Business employee signature with Key File issued by each Issuing CA
- Revoked NemID for Business employee signature with HW issued by each Issuing CA

Are several types of revocation list used (CRL Full, Partial CRL and OCSP), test is carried out in all used revocation list types.

Test scenario:

- Log on to the service provider's site
- Sign supported types of documents
  - Text
  - XML
  - HTML
  - PDF

Status after the test:

- Employee is not logged on service provider's website and can't sign the documents

10.4 Citizen with a valid NemID log on and sign

Test Objective:

- That a citizen with a valid NemID can log on to service provider's site and sign a document

Prerequisites:

- Service Provider Site that works

To be tested with the following certificates:

- Valid NemID with Key Card (OTP) issued by each Issuing CA
- Valid NemID for Hardware issued by each Issuing CA

Are several types of revocation list used (CRL Full, Partial CRL and OCSP), test is carried out in all used revocation list types.

Test scenario:

Log on to the service provider's site

Sign supported types of documents

- Text
- XML
- HTML
- PDF

Status after the test:

Citizen is logged on service provider's website and is able to sign documents

10.5 Citizen with a revoked NemID log on and sign

Test Objective:

- That an citizen with a revoked NemID is not able to log on to service provider's site and not able to sign documents

Prerequisites:

- Service Provider Site that works

To be tested with the following certificates:

- Revoked NemID with Key Card (OTP) issued by each Issuing CA
- Revoked NemID for Hardware issued by each Issuing CA

Are several types of revocation list used (CRL Full, Partial CRL and OCSP), test is carried out in all used revocation list types.

Test scenario:

- Log on to the service provider's site
- Sign supported types of documents
  - Text
  - XML
  - HTML
  - PDF

Status after the test:

- Citizen is not logged on service provider's website and can't sign the documents