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-nr. 30808460

Anbefalede testprocedurer

Indholdsfortegnelse

Versionsfortegnelse

24. februar 2010	Version 1.0	MOBO
22. marts 2010	Version 1.1	MTV
30. oktober 2010	Version 1.2	MTV
9. januar 2011	Version 1.3	MTV
15. oktober 2012	Version 1.4	MTVOL
19. marts 2014	Version 1.5	BMATZ

1 Formål og målgruppe

Dette dokument er en del af Tjenesteudbyderpakken for NemID.

Formålet med dokumentet er, at vejlede i hvordan tjeneste-udbyderen kan teste, om implementationen fungerer korrekt.

Dokumentet henvender sig til den ansvarlige for planlægning og udførelse af test hos tjenesteudbyderen.

Oversigt over alle dokumenter i Tjenesteudbyderpakken:

Overordnet dokumentation

- Introduktion til NemID og Tjenesteudbyderpakken
- Anbefalinger til interaktionsdesign og brugervalg af applet
- Drejebog for migrering til NemID
- Termer og begreber i NemID

Implementeringsdokumentation

- Implementeringsvejledning for NemID
- Konfiguration og opsætning

Testdokumentation

- Vejledning i brug af test tools
- **Anbefalede testprocedurer**

Referencedokumentation

- Specifikationsdokument for servicen PID-CPR
- Specifikationsdokument for servicen RID-CPR
- Specifikationsdokument for LDAP API
- Specifikationsdokument for OCSP
- Specifikationsdokument for OCES II

2 Test

Dette testdokument beskriver Nets DanIDs anbefalinger til de test, som tjenesteudbyderen bør gennemføre, inden der integreres mod Nets DanIDs produktionssystem.

Dokumentet beskriver først en række funktionelle områder der bør være gennemtestet inden de egentlige tests på use cases påbegyndes.

I tilfælde af fejl kan disse indrapporteres til Nets DanID på:

tu-support@danid.dk.

3 Funktionelle tests

Inden det use case-baserede testforløb påbegyndes, bør man sikre sig, at de mest basale dele af systemet er gennemtestet.

Herunder er nævnt de vigtigste områder for denne type test.

3.1 Generering og signering af applet parametre

Hvis appletten ikke er sat korrekt op lukker den ned og returnerer fejlkoden APP001 til tjenesteudbyderen.

Hvis appletten er sat korrekt op, kontakter den Nets DanIDs server og validerer, at opstartsparamenterne er korrekt signeret med et gyldigt VOCES certifikat og at Nets DanID har en aftale med det medsendte service provider ID. Hvis dette ikke er tilfældet, returnerer appletten fejlkoden SRV001 til tjenesteudbyderen.

Hvis appletten starter op og viser sit opstartsbillede med log-in er appletten sat korrekt op. Det eneste tjenesteudbyderen mangler at tjekke er, om dennes navn vises korrekt i appletten.

3.2 Modtage og validerer XMLDSig svar fra applet

Tjenesteudbyderens system skal kunne modtage det XMLDSig der bliver sendt til webserveren via de live connect call backs som appletten anvender.

Efterfølgende skal XMLDSig-svaret valideres for, om det er korrekt signeret.

3.3 Validerer certifikatet

For at validere certifikatet skal følgende skridt gennemføres:

1. Trække certifikatet ud af XMLDSig
2. Validere certifikatet og identificere CA som OCES I eller OCES II gennem hele certifikat-kæden til rodcertifikatet
3. Tjekke at certifikatet ikke er udløbet
4. Tjekke at certifikatet ikke er spærret

Hvis tjenesteudbyderen anvender sikkerhedspakken fra Nets DanID kan man nøjes med at validere om metoden i OOAPI returnerer et korrekt svar.

3.4 PID

Tjenesteudbyderen skal kunne trække PID ud af certifikatet.

Hvis tjenesteudbyderen anvender cpr-nr. til identifikation af brugeren skal PID-tjenesten bruges. Afhængig af anvendelsesmetode skal tjenesteudbyderen enten oversætte PID til cpr-nr. eller også lave et match-opslag på, om det af brugeren oplyste cpr-nr. matcher PID-nummeret.

Begge tests forudsætter, at tjenesteudbyderen har indgået særskilt aftale med Nets DanID om anvendelsen af PID-tjenesten.

3.5 RID

RID-tjenesten anvendes hvis der modtages MOCES medarbejder certifikater, hvor der er tilkoblet CPR-nr, og dette skal valideres.

4 NemID til Borger – log-in test cases

I det følgende er der beskrevet de vigtigste test cases du skal igennem for at sikre, at dit system er i stand til at anvende NemID til Borger og håndtere de mest almindelige borger-situationer.

4.1 Bruger med NemID logger på første gang

Dette er en positiv test der er succesfuldt gennemført, når brugeren er logget på tjenesteudbyderens selvbetjeningsunivers med NemID med nøglekort/nøgleviser.

1. Brugeren går ind på tjenesteudbyderens webside for at logge på dennes selvbetjeningsunivers.
2. Brugeren lokaliserer log-in knappen eller tilsvarende link, som der klikkes på.
3. Siden skifter over til log-in websiden med NemID og Digital Signatur.
4. Det er første gang at brugeren tilgår websiden og har derfor ikke nogen cookie liggende. Der defaultes til NemID tab.
5. Systemet lægger en cookie på brugerens computer.
6. Brugeren taster sit bruger-id
7. Brugeren indtaster sin adgangskode
8. Systemet anmoder brugeren om et fire cifret nøglenummer (#) på brugerens nøglekort.
9. Brugeren indtaster sin 6 cifrede nøgle fra nøglekortet.
10. Websiden skifter til tjenesteudbyderens selvbetjeningsunivers, hvor brugeren er identificeret.

4.2 Bruger med NemID kun til bank logger på

Dette er en negativ test, der er succesfuldt gennemført, når brugeren med NemID med nøglekort/nøgleviser er afvist fra at logge på tjenesteudbyderens selvbetjeningsunivers og har fået en fejlbesked med link til www.nemid.nu.

1. Brugeren går ind på tjenesteudbyderens webside for at logge på dennes selvbetjeningsunivers.

2. Brugeren lokaliserer log-in knappen eller tilsvarende link, som der klikkes på.

3. Websiden skifter og log-in billedet til NemID træder frem på skærmen.

4. Brugeren taster sit bruger-id

5. Brugeren indtaster sin adgangskode

6. Systemet returnerer med en fejlkode til tjenesteudbyderen.

7. Tjenesteudbyderen præsenterer fejl teksten for fejlkode OCES001 og brugeren henvises til www.nemid.nu.

4.3 Bruger med spærret (tidslåst) NemID logger på

Dette er en negativ test, der er succesfuldt gennemført, når brugeren med NemID med nøglekort/nøgleviser er afvist fra at logge på tjenesteudbyderens selvbetjeningsunivers og har fået en fejlbesked i applet.

1. Brugeren går ind på tjenesteudbyderens webside for at logge på dennes selvbetjeningsunivers.
2. Brugeren lokaliserer log-in knappen eller tilsvarende link, som der klikkes på.
3. Websiden skifter og log-in billedet til NemID træder frem på skærmen.
4. Brugeren taster sit bruger-id
5. Brugeren indtaster sin adgangskode
6. Systemet præsenterer en fejltekst i appletten, om at brugeren ikke kan logge på før tidslåsen er ophævet.
7. Systemet returnerer med fejlkode AUTH004 til tjenesteudbyderen.
8. Tjenesteudbyderen kan præsentere noget tekst for brugeren ved fejlkode AUTH004.

4.4 Bruger med låst (permanent) NemID logger på

Dette er en negativ test, der er succesfuldt gennemført, når brugeren med NemID med nøglekort/nøgleviser er afvist fra at logge på tjenesteudbyderens selvbetjeningsunivers og har fået en fejlbesked med link til support på www.nemid.nu.

1. Brugeren går ind på tjenesteudbyderens webside for at logge på dennes selvbetjeningsunivers.

2. Brugeren lokaliserer log-in knappen eller tilsvarende link, som der klikkes på.

3. Websiden skifter og log-in billedet til NemID træder frem på skærmen.

4. Brugeren taster sit bruger-id

5. Brugeren indtaster sin adgangskode

6. Systemet præsenterer en fejltekst i appletten om at brugeren ikke kan logge på, fordi dennes NemID er spærret.

7. Systemet returnerer med fejlkode AUTH005 til tjenesteudbyderen.

8. Tjenesteudbyderen præsenterer fejlteksten for fejlkode AUTH005 og brugeren henvises til support på www.nemid.nu.

4.5 Bruger med NemID på hardware logger på

Dette er en positiv test der er succesfuldt gennemført, når brugeren er logget på tjenesteudbyderens selvbetjeningsunivers med NemID på hardware (POCES II).

1. Brugeren går ind på tjenesteudbyderens webside for at logge på dennes selvbetjeningsunivers.
2. Brugeren lokaliserer log-in knappen eller tilsvarende link, som der klikkes på.
3. Siden skifter over til log-in websiden med NemID, nøglefil og Digital Signatur.
4. Det er første gang at brugeren tilgår websiden og har derfor ikke nogen cookie liggende. Der defaultes til Digital Signatur tab eller Log på med nøglefil-tab (hardware).
5. Brugerens certifikater fremtræder på drop down boksen i log-in billedet til Digital Signatur.
6. Brugeren vælger det relevante certifikat.
7. Systemet anmoder brugeren som dennes adgangskode
8. Brugeren indtaster sin adgangskode
9. Websiden skifter til tjenesteudbyderens selvbetjeningsunivers, hvor brugeren er identificeret.

4.6 Bruger med spærret NemID på hardware logger på

Dette er en negativ test, der er succesfuldt gennemført, når brugeren med Digital signatur eller NemID på hardware er afvist fra at logge på tjenesteudbyderens selvbetjeningsunivers.

1. Brugeren går ind på tjenesteudbyderens webside for at logge på dennes selvbetjeningsunivers.
2. Brugeren lokaliserer log-in knappen eller tilsvarende link, som der klikkes på.
3. Siden skifter over til log-in websiden med NemID, nøglefil og Digital Signatur.
4. Der defaultes til Digital Signatur tab eller Log på med nøglefil-tab (hardware).
5. Brugerens certifikater fremtræder på drop down boksen i log-in billedet til Digital Signatur.
6. Brugeren vælger det relevante certifikat.
7. Systemet anmoder brugeren som dennes adgangskode
8. Brugeren indtaster sin adgangskode
9. Tjenesteudbyder præsenterer brugeren for en fejltekst om at brugeren ikke kan logge på, fordi dennes NemID på hardware er spærret.

5 NemID til Borger – signering test cases

Tjenesteudbyderen skal validere, at den signerede tekst vises korrekt i appletten.

De test cases der er defineret i afsnit 4 for log-in, kan også være relevante for signering. Udgangspunktet er, at den samme signatur der er anvendt ved log-in også skal anvendes ved signering. I det tilfælde er disse test allerede gennemført ved test af log-in funktionen.
Det er dog sådan, at man som tjenesteudbyder ikke nødvendigvis kræver at brugeren først er logget på, før en tekst signeres. I denne situation er det Nets DanIDs anbefaling, at man også gennemfører de test cases, der er beskrevet under log-in.

5.1 Bruger signerer tekst skrevet i klartekst med NemID med nøglekort/nøgleviser

Dette er en positiv test, der er succesfuldt gennemført, når tjenesteudbyderen har valideret, at den signerede tekst i svaret fra appletten er identisk med den tekst der blev sendt til signering.

1. Brugeren går ind på tjenesteudbyderens webside og vælger den funktion, der kræver, at han signerer en tekst.
2. Tjenesteudbyderen sender den ønskede tekst til appletten som parameter.
3. Websiden skifter og signerings-billedet til signering med NemID vises på skærmen.
4. Brugeren validerer, at teksten er præsenteret korrekt.
5. Brugeren taster sit bruger-id
6. Brugeren indtaster sin adgangskode
7. Systemet anmoder brugeren om et fire cifret nøglenummer (#) på brugerens nøglekort.
8. Brugeren indtaster sin 6 cifrede nøgle fra nøglekortet.
9. Systemet returner den signerede svartekst til tjenesteudbyderen.
10. Tjenesteudbyderen validerer at svarteksten er identisk med den tekst, der blev givet til appletten i punkt 2.

5.2 Bruger signerer tekst skrevet i HTML med NemID med nøglekort/nøgleviser

Dette er en positiv test, der er succesfuldt gennemført, når tjenesteudbyderen har valideret, at den signerede tekst i svaret fra appletten er identisk med den tekst der blev sendt til signering.

1. Brugeren går ind på tjenesteudbyderens webside og vælger den funktion der kræver, at han signerer en tekst.
2. Tjenesteudbyderen sender den ønskede tekst til appletten som parameter.
3. Websiden skifter og signeringsbilledet til signering med NemID træder frem på skærmen.
4. Brugeren validerer, at teksten er præsenteret korrekt. Her er anvendt HTML, og det er vigtigt at de formateringsmuligheder som tjenesteudbyderen ønsker anvendt også præsenteres som forventet.
5. Brugeren taster sit bruger-id
6. Brugeren indtaster sin adgangskode
7. Systemet anmoder brugeren om et fire cifret nøglenummer (#) på brugerens nøglekort.
8. Brugeren indtaster sin 6 cifrede nøgle fra nøglekortet.
9. Systemet returner den signerede svartekst til tjenesteudbyderen.
10. Tjenesteudbyderen validerer, at svarteksten er identisk med den tekst der blev givet til appletten i punkt 2.

5.3 Bruger signerer tekst skrevet i XML med NemID med nøglekort/nøgleviser

Dette er en positiv test, der er succesfuldt gennemført, når tjenesteudbyderen har valideret, at den signerede tekst i svaret fra appletten er identisk med den tekst der blev sendt til signering.

1. Brugeren går ind på tjenesteudbyderens webside og vælger den funktion, der kræver, at han signerer en tekst.
2. Tjenesteudbyderen sender den ønskede tekst til appletten som parameter.
3. Websiden skifter og signeringsbilledet til signering med NemID vises på skærmen.
4. Brugeren validerer, at teksten er præsenteret korrekt. Her er anvendt XML, og det er vigtigt at de formateringsmuligheder som tjenesteudbyderen ønsker anvendt også præsenteres som forventet.
5. Brugeren taster sit bruger-id
6. Brugeren indtaster sin adgangskode
7. Systemet anmoder brugeren om et fire cifret nøglenummer (#) på brugerens nøglekort.
8. Brugeren indtaster sin 6 cifrede nøgle fra nøglekortet.
9. Systemet returner den signerede svar tekst til tjenesteudbyderen.
10. Tjenesteudbyderen validerer, at svarteksten er identisk med den tekst der blev givet til appletten i punkt 2.
11. Tjenesteudbyderen validerer, at svaret også indeholder information om det style sheet der blev brugt ved signeringen.

5.4 Bruger signerer PDF dokument med NemID med nøglekort/nøgleviser

Dette er en positiv test, der er succesfuldt gennemført, når tjenesteudbyderen har valideret, at den signerede tekst i svaret fra appletten er identisk med den tekst der blev sendt til signering.

1. Brugeren går ind på tjenesteudbyderens webside og vælger den funktion, der kræver, at han signerer en PDF.

2. Tjenesteudbyderen sender den ønskede PDF til appletten som parameter.
3. Websiden skifter og signeringsbilledet til signering med NemID vises på skærmen.
4. Brugeren validerer, at dokumentet er præsenteret korrekt.
5. Brugeren taster sit bruger-id
6. Brugeren indtaster sin adgangskode
7. Systemet anmoder brugeren om et fire cifret nøglenummer (#) på brugerens nøglekort.
8. Brugeren indtaster sin 6 cifrede nøgle fra nøglekortet.
9. Systemet returner den signerede svar tekst til tjenesteudbyderen.
10. Tjenesteudbyderen validerer, at svarteksten er identisk med den tekst der blev givet til appletten i punkt 2.

5.5 Bruger signerer tekst skrevet i klartekst med NemID på hardware

Dette er en positiv test, der er succesfuldt gennemført, når tjenesteudbyderen har valideret, at den signerede tekst i svaret fra appletten er identisk med den tekst der blev sendt til signering.

1. Brugeren går ind på tjenesteudbyderens webside og vælger den funktion der kræver, at han signerer en tekst.
2. Tjenesteudbyderen sender den ønskede tekst til appletten som parameter.
3. Websiden skifter og signeringsbilledet til signering NemID på hardware træder frem på skærmen.
4. Brugeren validerer, at teksten er præsenteret korrekt.
5. Brugerens certifikater fremtræder på drop down boksen i log-in billedet til NemID på hardware.
6. Brugeren vælger det relevante certifikat.
7. Systemet anmoder brugeren som dennes adgangskode
8. Brugeren indtaster sin adgangskode
9. Systemet returner den signerede svartekst til tjenesteudbyderen.
10. Tjenesteudbyderen validerer, at svarteksten er identisk med den tekst der blev givet til appletten i punkt 2.

5.6 Bruger signerer tekst skrevet i HTML med NemID på hardware

Dette er en positiv test, der er succesfuldt gennemført, når tjenesteudbyderen har valideret, at den signerede tekst i svaret fra appletten er identisk med den tekst der blev sendt til signering.

1. Brugeren går ind på tjenesteudbyderens webside og vælger den funktion der kræver, at han signerer en tekst.
2. Tjenesteudbyderen sender den ønskede tekst til appletten som parameter.
3. Websiden skifter og signeringsbilledet til signering med NemID på hardware træder frem på skærmen.
4. Brugeren validerer, at teksten er præsenteret korrekt. Her er anvendt HTML, og det er vigtigt at de formateringsmuligheder som tjenesteudbyderen ønsker anvendt også præsenteres som forventet.
5. Brugerens certifikater fremtræder på drop down boksen i log-in billedet til Digital Signatur.
6. Brugeren vælger det relevante certifikat.
7. Systemet anmoder brugeren som dennes adgangskode
8. Brugeren indtaster sin adgangskode
9. Systemet returner den signerede svartekst til tjenesteudbyderen.
10. Tjenesteudbyderen validerer, at svarteksten er identisk med den tekst der blev givet til appletten i punkt 2.

5.7 Bruger signerer tekst skrevet i XML NemID på hardware

Dette er en positiv test, der er succesfuldt gennemført, når tjenesteudbyderen har valideret, at den signerede tekst i svaret fra appletten er identisk med den tekst der blev sendt til signering.

1. Brugeren går ind på tjenesteudbyderens webside og vælger den funktion, der kræver, at han signerer en tekst.
2. Tjenesteudbyderen sender den ønskede tekst til appletten som parameter.
3. Websiden skifter og signeringsbilledet til signering med NemID på hardware vises på skærmen.
4. Brugeren validerer, at teksten er præsenteret korrekt. Her er anvendt XML, og det er vigtigt at de formateringsmuligheder som tjenesteudbyderen ønsker anvendt også præsenteres som forventet.
5. Brugerens certifikater fremtræder på drop down boksen i log-in billedet til Digital Signatur.
6. Brugeren vælger det relevante certifikat.
7. Systemet anmoder brugeren som dennes adgangskode
8. Brugeren indtaster sin adgangskode
9. Systemet returner den signerede svartekst til tjenesteudbyderen.
10. Tjenesteudbyderen validerer, at svarteksten er identisk med den tekst der blev givet til appletten i punkt 2.

6 NemID til Borger – Øvrige test cases

For NemID til Borger anbefales det at man som tjenesteudbyder tester sin implementering ved at gennemgå nedenstående test cases.

6.1 Bruger med MOCES II og log-in på borgerdel

Har man som tjenesteudbyder besluttet at man kun ønsker log-in og signering med personidentiteter og ikke erhvervsidentiteter bør man også teste at dette er sat rigtigt op, ved at forsøge at logge på med en erhvervssignatur. Resultatet skulle gerne være at vedkommende ikke får lov at logge på.

7 NemID til Erhverv – log-in test cases

For NemID til Erhverv anbefales det at man som tjenesteudbyder tester sin implementering ved at gennemgå nedenstående log-in test cases.

7.1 Bruger med NemID (Nøglekort) logger på

Testformålet:

At medarbejder med en valid NemID Erhverv medarbejdersignatur med Nøglekort kan logge på tjenesteudbyders site

Forudsætninger:

Tjenesteudbydersite der fungerer (Offentlig) Valid NemID Erhverv medarbejdersignatur med Nøglekort

Testforløb:

Login

Status efter test:

Medarbejder er logget på tjenesteudbyders website

7.2 Bruger med NemID (Softwarecertifikat) logger på

Testformålet:

At medarbejder med en valid NemID Erhverv nøglefil/softwarecertifikat kan logge på tjenesteudbyders site

Forudsætninger:

Tjenesteudbydersite der fungerer (Offentlig)

Medarbejder med et valid NemID Erhverv nøglefil/softwarecertifikat

Testforløb:

Login

Status efter test:

Medarbejder er logget på tjenesteudbyders website

7.3 Bruger med Digital Signatur (Medarbejdersignatur) logger på

Testformålet:

At medarbejder med en valid digital signatur kan logge ind på tjenesteudbyders site

Forudsætninger:

Tjenesteudbydersite der fungerer (Offentlig)

Medarbejder med valid digital signatur

Testforløb:

Login

Status efter test:

Medarbejderen er logget ind på tjenesteudbyder site

7.4 Bruger med tidslåst NemID (Nøglekort) logger på

Testformålet:

At medarbejder med en tidslåst NemID Erhverv medarbejdersignatur med Nøglekort ikke kan logge på tjenesteudbyders site

Forudsætninger:

Tjenesteudbydersite der fungerer (Offentlig)

Medarbejder med en tidslåst NemID Erhverv medarbejdersignatur med Nøglekort

Testforløb:

Login

Status efter test:

Medarbejder er ikke logget på tjenesteudbyders website

7.5 Bruger med spærret NemID (Nøglekort) logger på

Testformålet:

At medarbejder med en spærret NemID Erhverv medarbejdersignatur med Nøglekort ikke kan logge på tjenesteudbyders site

Forudsætninger:

Tjenesteudbydersite der fungerer (Offentlig)

Medarbejder med en spærret NemID Erhverv medarbejdersignatur med Nøglekort

Testforløb:

Login

Status efter test:

Medarbejder er ikke logget på tjenesteudbyders website

7.6 Bruger med spærret NemID (Softwarecertifikat) logger på

Testformålet:

At medarbejder med en Spærret NemID Erhverv nøglefil/softwarecertifikat ikke kan logge på tjenesteudbyders site

Forudsætninger:

Tjenesteudbydersite der fungerer (Offentlig)

Medarbejder med et spærret NemID Erhverv nøglefil/softwarecertifikat

Testforløb:

Login

Status efter test:

Medarbejder ikke er logget på tjenesteudbyders website

7.7 Bruger med spærret Digital Signatur (Medarbejdersignatur) logger på

Testformålet:

At medarbejder med en spærret Digital Signatur (Medarbejdersignatur) ikke kan logge ind på tjenesteudbyders site

Forudsætninger:

Tjenesteudbydersite der fungerer (Offentlig)

Medarbejder med spærret Digital Signatur (Medarbejdersignatur)

Testforløb:

Login

Status efter test:

Medarbejder kan ikke logge ind på tjenesteudbyder site

8 NemID til Erhverv – Signering test cases

For NemID til Erhverv anbefales det at man som tjenesteudbyder tester sin implementering ved at gennemgå nedenstående signering test cases.

8.1 Bruger med NemID (Nøglekort) signerer tekst

Det anbefales at teste signering af tekst skrevet i:

- Klar tekst
- HTML
- XML
- PDF

Testformålet:

At medarbejder med en valid NemID Erhverv medarbejdersignatur med Nøglekort kan signere henholdsvis klar tekst, HTML og XML på tjenesteudbyders site

Forudsætninger:

Tjenesteudbydersite der fungerer (Offentlig)

Medarbejder med en valid NemID Erhverv medarbejdersignatur med NøglekortTestforløb:

Signing

Status efter test:

Medarbejder kan signere på tjenesteudbyders website

8.2 Bruger med NemID (Softwarecertifikat) signerer tekst

Det anbefales at teste signering af tekst skrevet i:

- Klar tekst
- HTML

- XML
- PDF

Testformålet:

At medarbejder med en valid NemID Erhverv nøglefil/softwarecertifikat kan signere henholdsvis klar tekst, HTML og XML på tjenesteudbyders site

Forudsætninger:

Tjenesteudbydersite der fungerer (Offentlig)

Medarbejder med en valid NemID Erhverv nøglefil/softwarecertifikat

Testforløb:

Signing

Status efter test:

Medarbejder kan signere på tjenesteudbyders website

8.3 Bruger med Digital Signatur (Medarbejdersignatur) signerer tekst

Det anbefales at teste signering af tekst skrevet i:

- Klar tekst
- HTML
- XML
- PDF

Testformålet:

At medarbejder med en valid Digital Signatur (Medarbejdersignatur, OCES1) kan signere henholdsvis klar tekst, HTML og XML på tjenesteudbyders site

Forudsætninger:

Tjenesteudbydersite der fungerer (Offentlig)

Medarbejder med en valid Digital Signatur (Medarbejdersignatur)

Testforløb:

Signering

Status efter test:

Medarbejder kan signere på tjenesteudbyders website

9 NemID til Erhverv – Øvrige test cases

For NemID til Erhverv anbefales det at man som tjenesteudbyder tester sin implementering ved at gennemgå nedenstående test cases.

9.1 Bruger med POCES II og log-in på erhvervsdel

Har man som tjenesteudbyder besluttet at man kun ønsker log-in og signering med erhvervsidentiteter og ikke personidentiteter bør man også teste at dette er sat rigtigt op, ved at forsøge at logge på med en personsignatur. Resultatet skulle gerne være at vedkommende ikke får lov at logge på.

10 Multiple Issuing CA – test cases

I forbindelse med at der er implementeret flere Issuing CA'ere, er det relevant at teste at certifikater udstedt af hver Issuing CA håndteres korrekt. Dette gøres ved at NemID funktionaliteten testes med certifikater udstedt fra hver enkelt Issuing CA.

10.1 Opret testcertifikater

Da testcertifikater som udgangspunkt udstedes fra den aktive CA i testmiljøet (PP), er der behov for at gøre følgende for at udstede testcertifikater fra andre CA'er:

Ved testcertifikatudstedelse skal nedenstående indgå som en del af borgerens/medarbejderens certifikat navn (består certifikat navnet af andet end nedenstående skal det adskilles af mellemrum).

- Hvis "selectca-ica" indgår i certifikat navnet vil disse blive udstedt fra "den aktive CA" (default udstedende CA).
- Hvis "selectca-ocai" indgår i certifikat navnet vil disse blive udstedt fra den næst nyeste CA
- Hvis "selectca-ocaii" indgår i certifikat navnet vil disse blive udstedt fra den 3. nyeste CA osv.

Bemærk at selectca navne skal være uden "".

Pr. marts 2014 er to issuing CAer implementeret. Ica (den nye CA) og ocai (den gamle CA).

10.2 Medarbejder med NemID Erhverv logger på og signerer

Testformål:

- At medarbejder med en valid NemID Erhverv signatur kan logge på tjenesteudbyders site og kan signere et dokument

Forudsætninger:

- Tjenesteudbydersite der fungerer

Testes med følgende certifikater:

- Valid NemID Erhverv medarbejdersignatur med Nøglekort udstedt af hver issuing CA
- Valid NemID Erhverv medarbejdersignatur med Nøglefil udstedt af hver issuing CA

- Valid NemID Erhverv medarbejdersignatur med HW udstedt af hver issuing CA

Benyttes flere spærrelistetyper (Full CRL, Partial CRL og OCSP) foretages test i alle benyttede spærrelistetyper.

Testforløb:

- Login på tjenesteudbyders site
- Gennemfør signering af de understøttede dokumenttyper
  - Text
  - XML
  - HTML
  - PDF

Status efter test:

- Medarbejder er logget på tjenesteudbyders website og har signeret et dokument

10.3 Medarbejder med spærret NemID logger på og signerer

Testformål:

- At medarbejder med en spærret NemID Erhverv certifikat ikke kan logge på tjenesteudbyders site og ikke kan signere et dokument

Forudsætninger:

- Tjenesteudbydersite der fungerer

Testes med følgende certifikater:

- Spærret NemID Erhverv medarbejdersignatur med Nøglekort udstedt af hver issuing CA.
- Spærret NemID Erhverv medarbejdersignatur med Nøglefil udstedt af hver issuing CA.
- Spærret NemID Erhverv medarbejdersignatur med HW udstedt af hver issuing CA.

Benyttes flere spærrelistetyper (Full CRL, Partial CRL og OCSP) foretages test i alle benyttede spærrelistetyper.

Testforløb:

- Login på tjenesteudbyders site
- Gennemfør signering af de understøttede dokumenttyper
  - Text

  - XML
  - HTML
  - PDF

Status efter test:

- Medarbejder er ikke logget på tjenesteudbyders website og har ikke kunne signere dokumenter

10.4 Borger med NemID logger på og signerer

Testformål:

- At borger med en valid NemID signatur kan logge på tjenesteudbyders site og kan signere et dokument

Forudsætninger:

- Tjenesteudbydersite der fungerer (Offentlig)

Testes med følgende certifikater:

- Valid NemID Borger signatur med OTP udstedt af hver issuing CA
- Valid NemID Borger signatur med HW udstedt af hver issuing CA

Benyttes flere spærrelistetyper (Full CRL, Partial CRL eller OCSP) foretages test i alle benyttede spærrelistetyper.

Testforløb:

- Login på tjenesteudbyders site
- Gennemfør signering af de understøttede dokumenttyper
  - Text
  - XML
  - HTML
  - PDF

Status efter test:

- Borger er logget på tjenesteudbyders website og kan signere dokumenterne

10.5 Borger med spærret NemID logger på

Testformål:

- At borger med en spærret NemID signatur ikke kan logge på tjenesteudbyders site og ikke kan signere et dokument

Forudsætninger:

- Tjenesteudbydersite der fungerer (Offentlig)

Testes med følgende certifikater:

- Spærret NemID Borger signatur med OTP udstedt af hver issuing CA
- Spærret NemID Borger signatur med HW udstedt af hver issuing CA

  Benyttes flere spærrelistetyper (Full CRL, Partial CRL og OCSP) foretages test i alle benyttede spærrelistetyper.

Testforløb:

- Login på tjenesteudbyders site
- Gennemfør signering af de understøttede dokumenttyper
  - Text
  - XML
  - HTML
  - PDF

Status efter test:

- Borger er ikke logget på tjenesteudbyders website og kan ikke signere dokumenter