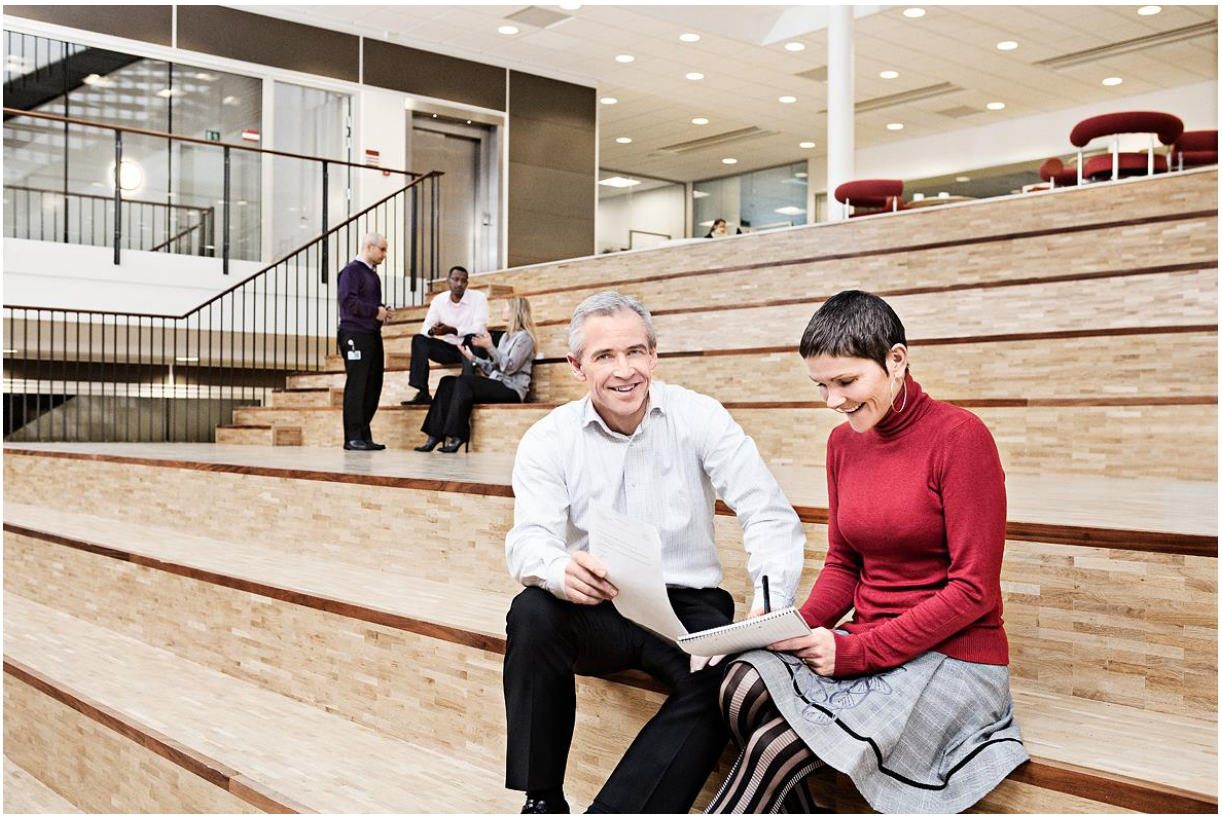


Digitaliseringsstyrelsen

Nemlog-in
Vejledning

Beskrivelse af Leverandørens integrationstestmiljø

Version: 2.d

ID: 32309

2018-07-03

NNIT
Conscience driven. Value adding

Indhold

1 Introduktion

Nærværende dokument beskriver Leverandørens integrationstestmiljø (herefter kaldet testmiljø), som stilles til rådighed for serviceudbydere (myndigheder) i forbindelse med migreringstest og integrationstest via https://administration.nemlog-in.dk[1].

Testmiljøet kan indeholde kendte fejl og mangler, som skyldes det aktuelle build, der udgør testmiljøet. Der henvises til release information [4] for aktuelle opdateringer.

Testmiljøet stiller en vejledning til rådighed som hjælper serviceudbydere med at fejlsøge deres løsninger i gennemførsel af test. Der henvises til dokumentet hjælp til fejlsøgning af din løsning [5].

I dokumentet anvendes betegnelsen *service* om en løsning (fx en portal) der er tilsluttet af en serviceudbyder med henblik på integration med Nemlog-in SSO/SLO og signerings-tjeneste.

Dokumentet er struktureret således:

- Afsnit "Test af services" beskriver hvordan serviceudbydere anvender testmiljøet til at teste integration med Nemlog-in SSO/SLO.
- Afsnit "Tilslutning af service metadata" beskriver hvordan serviceudbydere skal tilslutte service metadata og Attribute Query funktionaliteten.
- Afsnit "Identity Provider" beskriver testmiljøets Identity Provider, som leverer Nemlog-in SSO/SLO.
- Afsnit "Metadatavalidator" beskriver anvendelsen af metadatavalidatoren, som skal benyttes til at verificere service metadata, før udveksling med Nemlog-in.
- Afsnit "Signeringstjenesten" beskriver hvordan serviceudbydere skal udvikle og teste integrationen mellem deres tjeneste og signeringstjenesten.
- Afsnit "Common domain cookie viewer" beskriver anvendelsen af common domain cookie viewer.
- Afsnit "Log viewer" beskriver anvendelsen af log viewer, som kan benyttes til at fejlsøge integration med Nemlog-in SSO/SLO.

På testmiljøets forside https://test-nemlog-in.dk/testportal/ findes links til værktøjer og dokumentation.

[1] https://administration.nemlog-in.dk er et administrativt system der automatiserer tilslutning af services herunder udveksling af metadata. En organisation skal være oprettet via migrering eller via https://tilslutning.nemlog-in.dk samt have en teknisk administrator tilknyttet før administrationsportalen kan benyttes.

2 Test af services

2.1 Nemlog-in SSO/SLO

Dette afsnit henvender sig til serviceudbydere, der ønsker at teste integration mellem deres services og Nemlog-in SSO/SLO.

2.1.1 Udveksling af metadata

Før serviceudbyder kan påbegynde test skal der udvekles metadata mellem service og Identity Provider.

1) **Service metadata migrerede services** vil automatisk blive migreret fra det nuværende Nemlog-in og importeret i testmiljøets Identity Provider. Serviceudbyder skal derfor ikke foretage sig yderligere i denne henseende, så længe at der ikke er tale om en ny version af servicen.
2) **Identity Provider metadata** er serviceudbyder ansvarlig for at importere i de respektive testmiljøer, hvor deres services findes installeret. Metadata skal importeres for hver service, der indgår i serviceudbyders test.
3) **Service metadata til en ny service eller ny version af service** skal opdateres igennem https://administration.nemlog-in.dk og være i "integrations test klar" tilstand før systemet vil være tilgængeligt for integrations test miljøet.

Identity Provider metadata kan downloades fra testmiljøets forside.

2.1.2 Testbrugere

Testmiljøet benytter sig af DanID's testmiljø og tillader derfor kun login med POCES og MOCES certifikater, der er udstedt herigennem.

Serviceudbyder skal selv sørge for at skaffe testcertifikater hos DanID, som tilbyder flere muligheder;

- På DanID's hjemmeside er det muligt at hente et begrænset antal præ-definerede testcertifikater [4].
- DanID stiller flere on-line værktøjer [2] til rådighed, som giver serviceudbyder mulighed for at danne egne certifikater, både som nøglefil og nøglekort.

Derudover stiller NNIT et begrænset antal testcertifikater til rådighed, som kan downloades fra testmiljøets forside. Der henvises til vejledning for testcertifikater [3].

2.1.3 Test Service Provider #1 (IdP-SP-side-1)

Test Service Provider der kan benyttes af serviceudbydere til test af SSO og SLO samspil med serviceudbyder services.

Link til test Service Provider forside: https://sp1.test-nemlog-in.dk/demo/. Forsiden benævnes herefter testside 1.

Testside 1 kan være i en af to tilstande afhængigt af, om bruger allerede har en aktiv session med Identity Provider (=logget ind via anden Service Provider).

2.1.3.1 Tilstand: bruger er ikke logget ind

Siden rummer følgende:

- En knap benævnt "Login" til at igangsætte login mod Identity Provider.
- En "Force" knap til at igangssætte login, hvor Identity Provider instrueres om altid at vise sin loginside, uanset om bruger allerede har en aktiv session med Identity Provider. Bruger vil derfor altid skulle logge ind igen.
- En knap benævnt "Passive" til at igangsætte login hvor Identity Provider instrueres om ikke at overtage brugergrænsefladen. Har bruger en aktiv session med Identity Provider, vil Identity Provider gennemføre SSO og returnere assertion til siden. Har bruger ikke en aktiv session, vil Identity Provider returnere en afledt statuskode, som præsenteres på siden.
- En "Logout" knap til at aktivere SLO, som igangsætter logout mod Identity Provider hvorefter alle serviceudbydere, brugeren aktuelt har en session med, vil blive kontaktet af Identity Provider med henblik på logout. Figur 2 nedenfor illustrerer indlogget bruger for testside 1.

Figur 1 nedenfor illustrerer testside 1 for ej indlogget bruger.

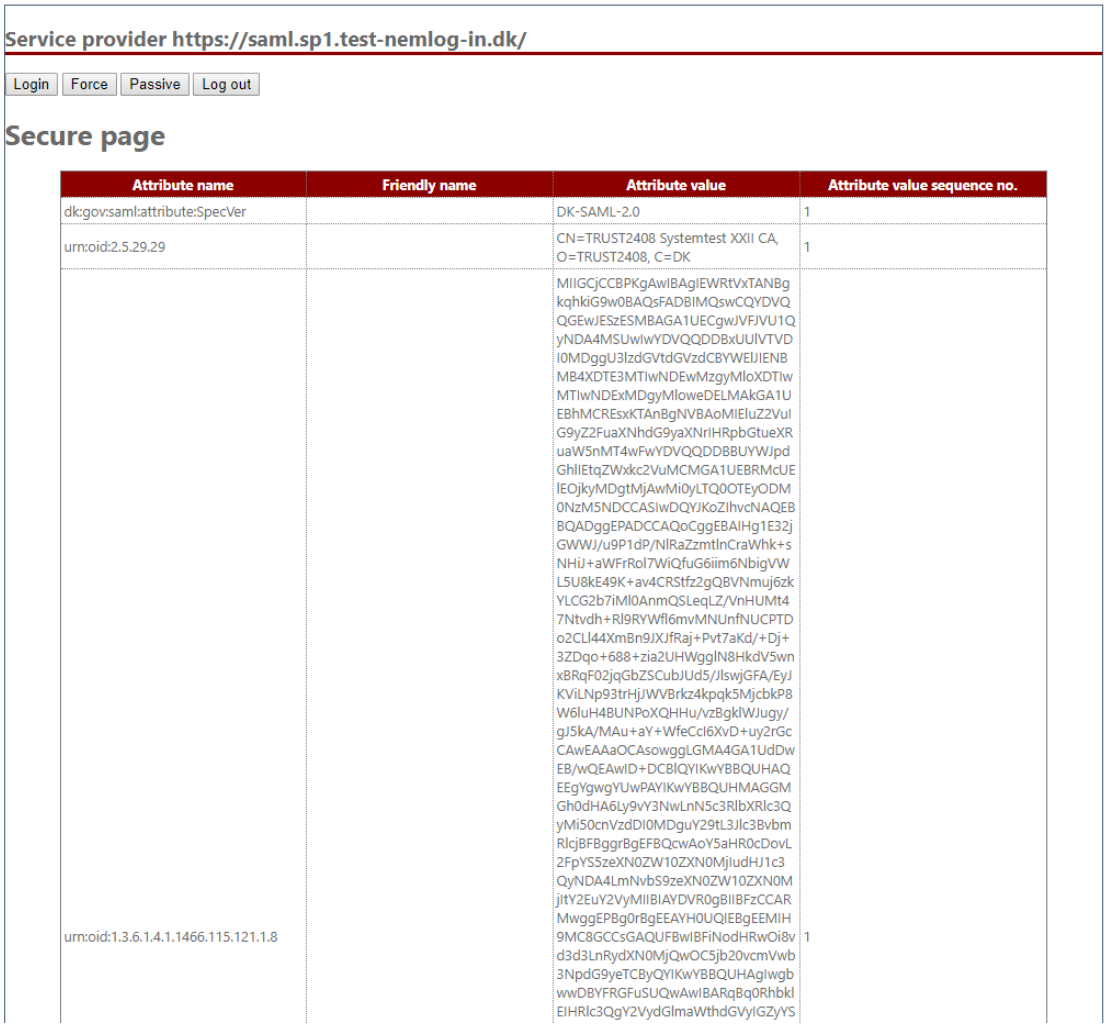
Figur 1: Testside 1, bruger ej indlogget

2.1.3.2 Tilstand: bruger er logget ind

Hvis bruger er logget ind, rummer siden følgende:

- Attributterne fra den modtagne SAML assertion fra Identity Provider. Testside 1 er konfigureret til at anvende OCES attributprofilen[2], hvilket er afspejlet i de viste attributter. Der henvises til OIO Web SSO Profile [1] for detaljer om attributprofilerne.
- Indholdet af Session values.
- En "Login" knap til at igangssætte login, hvor Identity Provider instrueres om ikke at overtage brugergrænsefladen. Har bruger en aktiv session med Identity Provider, vil Identity provider gennemføre en single sign-on og returnere assertion til siden. Har bruger ikke en aktiv session, vil Identity Provider igangsætte login.
- En "Force" knap til at igangssætte login, hvor Identity Provider instrueres om altid at vise sin loginside, uanset om bruger allerede har en aktiv session med Identity Provider. Bruger vil derfor altid skulle logge ind igen.
- En "Passive" knap til at igangsætte login hvor Identity Provider instrueres om ikke at overtage brugergrænsefladen. Har bruger en aktiv session med Identity Provider, vil Identity Provider gennemføre SSO og returnere assertion til siden. Har bruger ikke en aktiv session, vil Identity Provider returnere en afledt statuskode, som præsenteres på siden.
- En "Logout" knap til at aktivere SLO, som igangsætter logout mod Identity Provider hvorefter alle serviceudbydere, brugeren aktuelt har en session med, vil blive kontaktet af Identity Provider med henblik på logout. Figur 2 nedenfor illustrerer indlogget bruger for testside 1.

[2] Bemærk, at ikke alle attributter understøttes i denne version af Nemlog-in. Attributter anvendt i det nuværende Nemlog-in vil være understøttet.



Figur 2: Udsnit af testside 1, bruger er indlogget

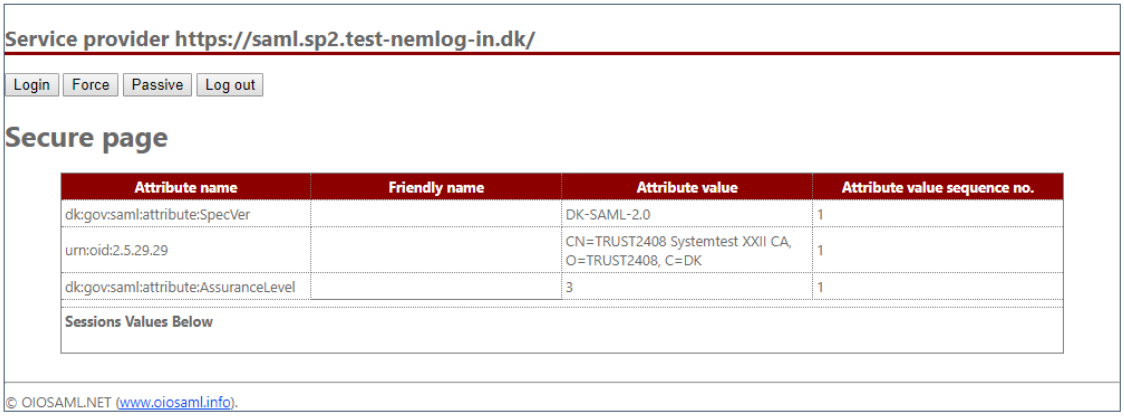
2.1.4 Test Service Provider #2 (IdP-SP-side-2)

Test Service Provider der kan benyttes af serviceudbydere til test af SSO og SLO samspil med serviceudbyder services.

Link til test Service Provider forside: https://sp2.test-nemlog-in.dk/demo/. Forsiden benævnes herefter testside 2.

Testside 2 er funktionel identisk med testside 1 bortset fra, at testside 2 er konfigureret til at benytte persistente pseudonymer. Det betyder, at det modtagne sæt af attributter i SAML assertion, er bestemt af Persistent Pseudonym Attribute Profile, som findes beskrevet i OIO Web SSO Profile [1].

Figur 3 nedenfor illustrerer indlogget bruger for testside 2.



Figur 3: Udsnit af testside 2, bruger er indlogget

3 Tilslutning af service metadata

3.1 Nemlog-in release1

3.1.1 Information omkring tilslutning af service metadata

For Nemlog-in release1 eksisterer der kun en type af IDP metadata: IDP metadata som dækker den nye standard OIO Profil "OIO Web SSO Profile". Service metadata som ønskes indlæst på Testmiljøet eller Produktionsmiljøet skal sendes til Digitaliseringsstyrelsen for udførsel af indlæsning.

3.2 Nemlog-in release2

3.2.1 Information omkring tilslutning af service metadata

Nemlog-in release2 indeholder https://administration.nemlog-in.dk, der er et administrativt system, der automatiserer tilslutning af services herunder udveksling af serviceudbydernes service metadata. Brugergrænsefladen for tilslutningssysstemet er kun tilgængeligt via Produktionsmiljøet.

For Nemlog-in release2 eksisterer der kun et type af IDP metadata - IDP metadata som dækker den standard OIO Profil "OIO Web SSO Profile".

Det er betingelsen at alle serviceudbydere integrere deres service op mod den standard "OIO Web SSO Profile".

3.2.1.1 For Testmiljøet

Det er muligt gennem tilslutningssystemet i Produktionsmiljøet at sende(provisionere) service metadata til test i Testmiljøet. Det at sende service metadata til test i Testmiljøet fra Produktionsmiljøet er i praksis et skridt i processen for at få godkendt en tilslutning af service metadata i Productionssystemet.

Testbrugere der skal have tilknyttet et eller flere privilegier i Testmiljøet, skal være oprettet og tilknyttet den relevante service via https://administration.nemlog-in.dk

Fordi serviceudbydere har denne mulighed, så har serviceudbyderne ikke længere muligheden for at sende service metadata til indlæsning gennem Digitaliseringsstyrelsen. Digitaliseringsstyrelsen vil dog forsat yde teknisk support på eventuelle problemer der skulle være med tilslutningen af service metadata som er sendt af tilslutningssystemet til Testmiljøet for at teste integrationen op Testmiljøet.

3.2.1.2 For Produktionsmiljøet

En serviceudbyder som ønsker at opdatere service metadata skal følge nedenstående fremgangsmetode. Serviceudbyder skal opdatere service metadata i tilslutningssystemet ved blot at lave en ny version af service metadata og tilføje de ønskede ændringer i attributerne.

For serviceudbydere som for første gang skal tilsluttes til Nemlog-in release2, så skal service metadata oprettes i tilslutningssystemet med OIO Profil "OIO Web SSO Profile".

3.2.2 Information omkring tilslutning af Attribute Query metadata

Med den Nemlog-in release2 åbnes der op for brugen af Attribute Query. En Attribute Query metadata autogenereres internt af Nemlog-in release2 systemet ved indlæsning af en service metadata i Testmiljøet eller ved tilslutning af service metadata gennem tilslutningssystemet i Productionsmiljøet.

Dette betyder, at for at få adgang til Attribute Query funktionaliteten, så skal en serviceudbyder derfor ikke fortage sig andet end at levere service metadata med OIO Profil "OIO Web SSO Profile" til indlæsning på Testmiljøet eller til tilslutning på Produktionsmiljøet gennem tilslutningssystemet.

4 Identity Provider

4.1 Nemlog-in release2

4.1.1 IDP-metadata for "OIO Web SSO Profile"

Testmiljøet rummer en Identity Provider "IDP-metadata (Testmiljø) (OIOSAML Basic privilege profile)" med følgende entity ID:

- **https://saml.test-nemlog-in.dk/**

Testmiljøets Identity Provider er funktionel identisk med den Identity Provider som stilles til rådighed i produktion. Identity Provider "IDP-metadata (Produktionsmiljø)" som stilles til rådighed i produktion har følgende entityID:

- **https://saml.nemlog-in.dk**

Herunder listes de væsentligste features som Identity Provider understøtter:

- Login / Single Sign-On.
- Login med ForceAuthn instruks.
- Login med IsPassive instruks.
- Persistent pseudonym og X.509 attributprofiler.
- Initierende Single logout (Request) fra Service Provider til Identity Provider med HTTP Redirect og POST bindinger.
- Efterfølgende Single logout (Request) fra Identity Provider til Service Provider med HTTP Redirect, HTTP POST og SOAP bindinger.
- Loginsiderne understøtter brug i iframe sider.
- Understøtter det fulde sæt af SAML attributer i relation til tilslutningssystemet (f.eks. attribut til beskrivelse af privilegier)
- Understøtter Attribute Query

4.2 Common domain cookie

Identity Provider indgår i common domain test-fobs.dk. Ved udført login af bruger, som ikke i forvejen har en aktiv session med Identity Provider, vil Identity Provider skrive sin identitet i den tilhørende commain domain cookie (CDC) i henhold til retningslinier beskrevet i OIO Web SSO Profile [1].

4.3 Valideringer af certifikat

Identity Provider foretager valideringer af certifikat anvendt ved login samt certifikat anvendt til signering af SAML beskeder.

Valideringer omfatter om certifikat er udløbet, om certifikat er udstedt af godkendt certifikatautoritet (CA) samt om certifikat er tilbagekaldt (revoked).

4.4 Integration med DanID's testmiljø

Identity Provider benytter DanID's testmiljø og dermed de tilhørende testudgaver af DanID's ressourcer samt DanID testdata. Det påvirker fx hvilke certifikater der kan anvendes ved login hos Identity Provider.

Der henvises til afsnittet om "Testbrugere".

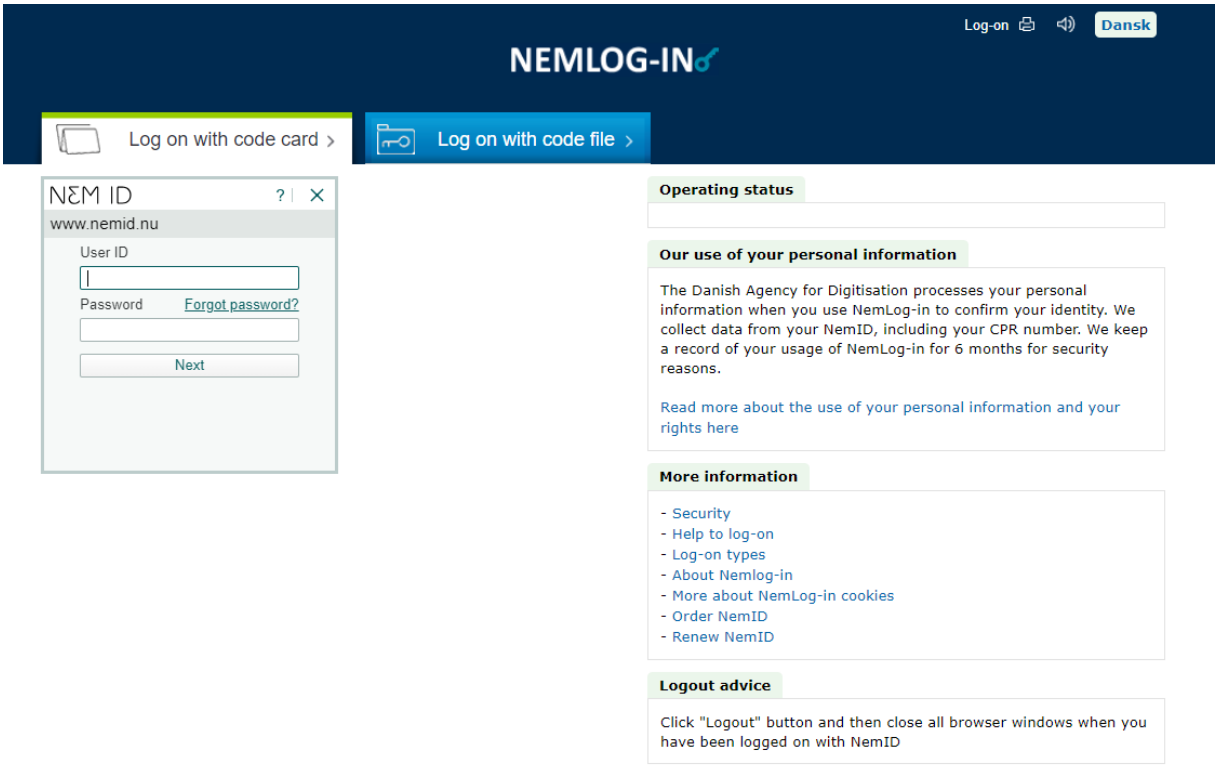
4.5 Brugergrænseflade

Identity Providers brugergrænseflade er identisk med den brugergrænseflade, som stilles til rådighed i produktion. Det er blandt andet her at Identity Provider loginsiden findes, hvor bruger har mulighed for at vælge mellem forskellige logintyper, svarende til de typer, der understøttes af DanID.

Bruger har gennem brugergrænsefladen mulighed for at;

- Fravælge Single Sign-On (Opt-out) således, at bruger altid mødes af loginside, uanset om bruger allerede har en aktiv session med Identity Provider.
- Vælge en default logintype, som herefter automatisk vises når bruger mødes af loginsiden.
- Ændre sprog mellem engelsk og dansk.

Figur 4 nedenfor illustrerer Identity Provider loginside.



Figur 4: Loginside

5 Metadatavalidator

Link: https://test-nemlog-in.dk/metadatavalidator/

Metadatavalidatoren giver serviceudbydere mulighed for at validere deres metadata før de udveksles med Nemlog-in, og som led i fejlsøgning såfremt, at metadata mistænkes som fejlkilden i test.

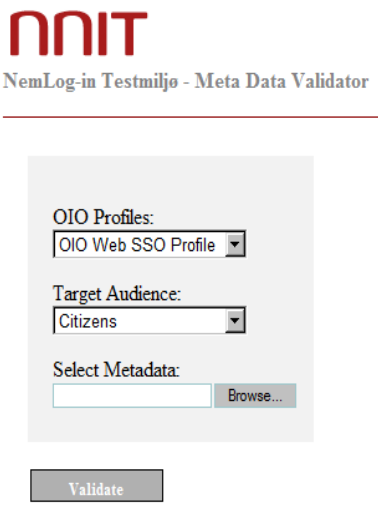
Metadatavalidatoren kontrollerer at metadata,

- Er i overenstemmelse med SAML 2.0 metadataskema.
- Er i overenstemmelse med politikker beskrevet i OIO Web SSO Profile [1].

Der kan foretages validering af metadata til både Nemlog-in's testmiljø og produktionsmiljø.

5.1 Start validering af metadata

Figur 5 nedenfor illustrerer metadatavalidatorens forside.



Figur 5: Metadatavalidator forside

Validering af metadata:

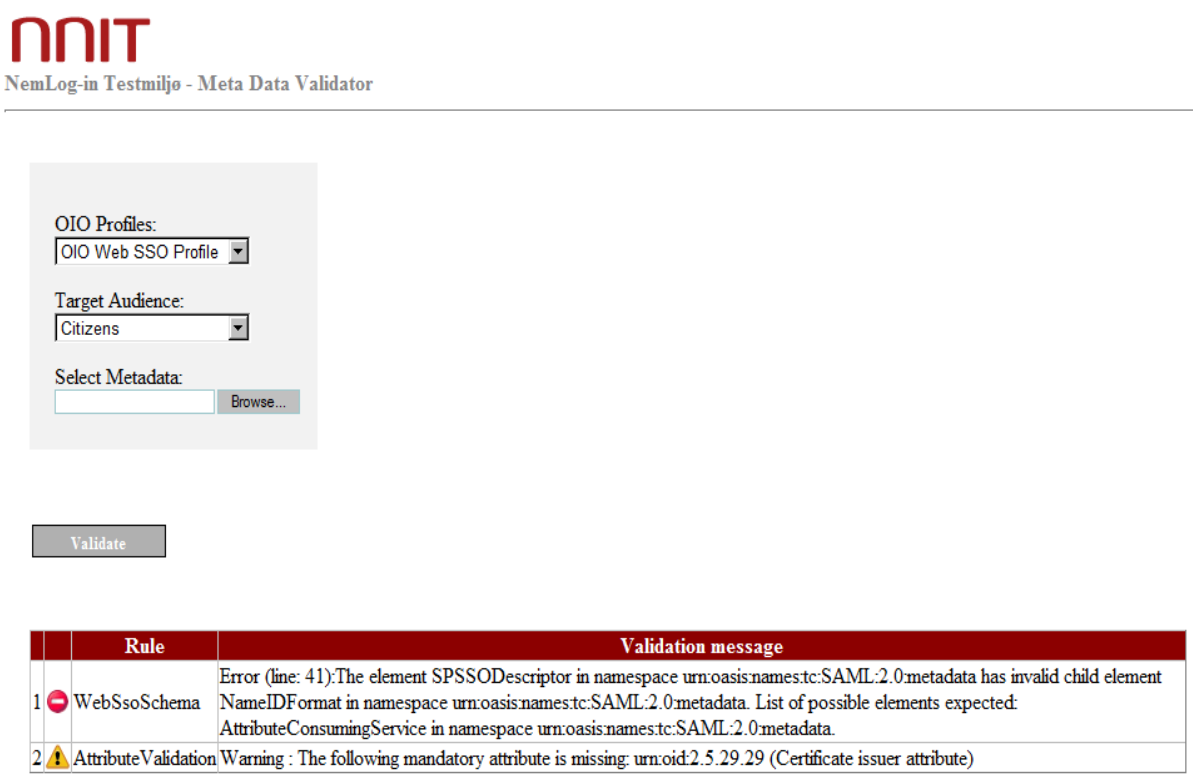
- I listen "OIO Profile" vælges den OIO Profil der ønskes at valideres imod. "OIO Web SSO Profile" vælges for validering af metadata iht. OIO Web SSO Profile [1].

Ydermere bør det her bemærkes, at "OIO Web SSO Profile" skal vælges for validering af både service metadata som integrerer op mod Nemlog-in release1 og Nemlog-in release2 (som indeholder det tidligere nævnte tilslutningssystem og Attribute Query).

- I listen "Target Audience" vælges om løsningen der valideres metadata for understøtter personcertifikater, medarbejdercertifikater eller begge. Korrekt angivelse af target audience sikrer, at erklærede attributter i metadata valideres iht. løsningens virke.
- Knappen "browse" vælges for at uploade metadatafil til validering.
- Knappen "Valider" vælges for at påbegynde validering.

5.2 Valideringsresultat

Figur 6 nedenfor illustrerer metadatavalidatorens resultatside.



Figur 6: Udsnit af metadatavalidator resultatside

Valideringsbeskeder vil blive præsenteret i en tabel, som det er illustreret i figur 7.

Resultat af validering:

- Første kolonne angiver fortløbent nummer for valideringsbesked (nummeret er en reference og har en ingen teknisk betydning).

- Anden kolonne indeholder ikon, som angiver om valideringsbesked betragtes som advarsel eller fejl.
- Kolonnen ”Rule” angiver valideringsreglen der er valideret for.
- Kolonnen ”Validation message” indeholder valideringsbeskeden. Evt. tal i parentes () henviser til linie i metadatafilen.

Sådan fortolkes valideringsbeskeder:

- Hvis ingen fejl eller advarsler er rapporteret kan metadata udveksles med Nemlog-in.
- Hvis der rapporteres advarsler (men ingen fejl) kan metadata som udgangspunkt udveksles med Nemlog-in til migreringstest[3]
- Hvis der rapporteres fejl kan metadata ikke udveksles med Nemlog-in.

[3] Metadata til produktion skal validere uden fejl eller advarsler.

6 Signeringstjenesten

Dette afsnit henvender sig til tjenesteudbydere, der ønsker at udvikle og teste integration mellem deres tjeneste og signeringstjenesten.

Signeringstjenesten kan aktiveres på to måder: Som web og som WCF servcice. For yderligere information om tjenesten henvises til signing service [7] dokumentet.

I integrationsmiljøet er Web tjenesten tilgængelig her:

POST: https://signering.test-nemlog-in.dk/signer.aspx

Og WCF tjenesten tilgængelig her:

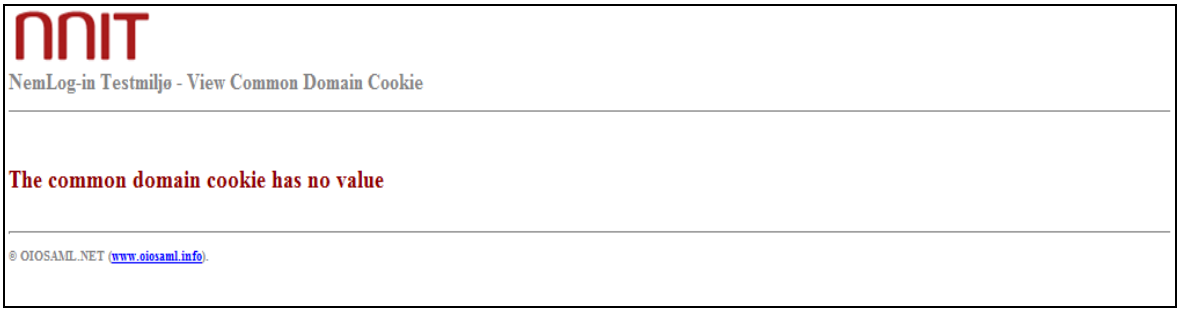
WCF: https://signingservice.signering.test-nemlog-in.dk/SigningService.svc

7 Common domain cookie viewer

Link: https://idp.test-fobs.dk/view.aspx

I forbindelse med login af bruger sætter Identity Provider indholdet af common domain cookie til Nemlog-in's entityID. Common domain cookie viewer viser indholdet af cookien.

Figur 7 nedenfor illustrerer common domain cookie viewer forside.



Figur 7: common domain cookie viewer forside

8 Log viewer

Link: https://test-nemlog-in.dk/logviewer/

Identity Provider foretager logninger af en række begivenheder (events) i forbindelse med udførelse af login og logout. Log viewer giver serviceudbydere mulighed for at fejlsøge gennem søgning i disse logninger.

Der henvises til log viewer vejledning [6] for yderligere detaljer.

9 Referencer

[1] OIO Web SSO Profile på digitaliser.dk.

[2] Vejledning i brug af test tools på nets-danid.dk.

[3] Pre-defined test certificates.

[4] Release information.

[5] Hjælp til fejlsøgning af din løsning.

[6] Log viewer vejledning.

[7] Signing service.

10 Ændringslog

Dato	Version	Beskrivelse af ændring	Initialer
2012-12-12	1.a	Dokument restruktureret og opdateret i forbindelse med release A go-live.	MWL
2012-12-14	2.0	Godkendt	MWL
2013-05-29	2.a	Dokument opdateret i forbindelse med release B myndighedstest migrering.	DDOL
2013-06-10	2.b	Opdateret i relation til signeringstjenesten.	ASEP
2013-06-12	2.c	Opdateret Attribute Query metadata afsnittet	DDOL
2018-07-03	2.d	Updated the document following the Release10	TZKM