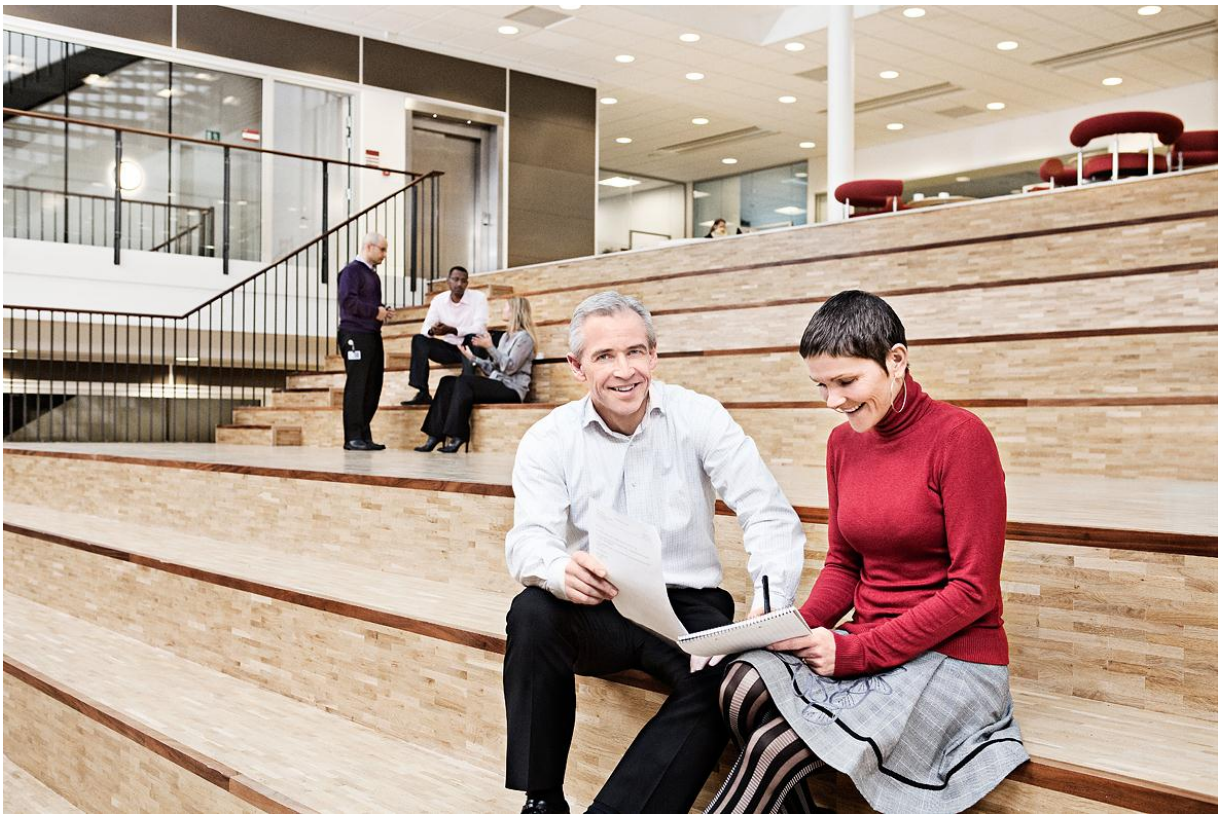

Digitaliseringsstyrelsen

Nemlog-in
Vejledning

Hjælp til fejlsøgning af din løsning

Version: 3.0

ID: 32309

2012-12-13

NNIT
Conscience driven. Value adding

Indholdsfortegnelse

1 Introduktion

Dette dokument beskriver typiske årsager til fejl der er observeret i forbindelse med test mod det nye Nemlog-in.

Hvis du har oplevet fejl i forbindelse med at få adgang til testmiljøet, kan det skyldes, at der er fejl i jeres test metadata, eller der ikke er registret test metadata for jeres løsning i NemLog-in.

Dokumentet kan hjælpe dig med:

- At verificere dine metadata før du udveksler dem med Nemlog-in. Der henvises til afsnit ”2. Verificering af metadata”.
- At forberede konfiguration af din løsning samt fejlsøge når du tester din løsning mod Nemlog-in. Der henvises til afsnit ”3. Min løsning fejler under login til Nemlog-in” og ”4. Min løsning fejler efter login i Nemlog-in”.

I dokumentet anvendelse betegnelsen *Nemlog-in1* for det eksisterende Nemlog-in. Det nye Nemlog-in refereres *Nemlog-in*.

2 Verificering af metadata

Mange af de observerede fejl kan tilbageføres til løsningers metadata der er udvekslet med Nemlog-in. Før du udveksler metadata for din løsning er det derfor en god ide, at kontrollere metadata for de beskrevne fejl i dette afsnit.

Bemærk at testmiljøet stiller en metadatavalidator til rådighed, som vil være i stand til at identificere flere af de beskrevne fejl. Der henvises til beskrivelse af testmiljø [1] for aktuel liste over tilgængelige testfaciliteter.

2.1 Benytter jeg det rigtige signeringscertifikat?

Kontrollér at signeringcertifikat i metadata,

- **Er det korrekte certifikat.** Certifikatet skal være identisk med det certifikat din løsning signerer AuthnRequest til Nemlog-in med.
- **Er gyldigt.** Certifikatets gyldighedsperiode er korrekt.
- **Har korrekt type.** Certifikatet skal være af typen VOCES eller FOCES.
- **Er udstedt af DanID's testmiljø Certificate Authority (CA), hvis metadata er rettet mod Nemlog-in testmiljøet.** Certifikatet skal være udstedt af "TDC OCES Systemtest CA II".
- **Er udstedt af DanID's produktionsmiljø Certificate Authority (CA), hvis metadata er rettet mod Nemlog-in produktionsmiljøet.** Certifikatet skal være udstedt af "TDC OCES CA" eller "TRUST2408 OCES CA".
- **Ikke er anvendt i flere løsninger.** Samme certifikat kan kun være registreret én gang i Nemlog-in.

Ovenstående betingelser gælder ligeledes for krypteringscertifikat. Bemærk at der for mange løsninger vil være sammenfald i signerings- og krypteringscertifikat.

2.2 Passer entityID med den løsning jeg arbejder med?

Kontrollér at entityID i metadata,

- Svarer til entityID til den løsning du skal igang med at teste eller sætte i produktion.
- Er entydigt for det Nemlog-in miljø metadata er rettet imod (testmiljø og produktionsmiljø).

Eksempel på entityID i erklæret metadata:

```
<md:EntityDescriptor entityID="https://sp1.test-nemlog-in.dk" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
```

Der henvises i øvrigt til OIOSAML Web SSO [2] for beskrivelse af navnekonvention og regler for entityID.

2.3 Skal jeg angive NameIDFormat?

Kontrollér at NameIDFormat i metadata er korrekt:

- Nemlog-in understøtter ”Persistent” og ”X509SubjectName”.

Eksempel på NameIDFormat erklæret i metadata:

```
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</md:NameIDFormat>
```

2.4 Attributten UniqueAccountKey

Attributten ” dk:gov:saml:attribute:UniqueAccountKey” understøttes ikke af Nemlog-in, i det dens implementation i OIOSAML Web SSO [2] ikke er endeligt defineret.

Hvis den angives i løsningers metadata vil Nemlog-in fejle som konsekvens.

Ovenstående adskiller sig fra Nemlog-in1, hvor attributten understøttes, men altid returneres tom.

3 Min løsning fejler under login til Nemlog-in

Din løsning sender et såkaldt AuthnRequest til Nemlog-in når en bruger ønsker at logge ind på din løsning via Nemlog-in. Fejl sket under login vil typisk være forårsaget af fejl i AuthnRequest.

Dette afsnit beskriver typiske AuthnRequest fejlsituationer der er observeret i forbindelse med test mod Nemlog-in. Afsnittet er rettet mod både nye løsninger og løsninger der migreres fra det nuværende Nemlog-in. Særligt for migrerede løsninger kan der opleves foreskelle i hvordan det nuværende Nemlog-in og Nemlog-in fortolker AuthnRequests.

Generelt kan det anbefales at AuthnRequests ikke indeholder erklæringer, som allerede er konfigureret i Nemlog-in gennem udveksling af løsningers metadata og som derfor typisk vil fejle, hvis der opstår konflikt mellem AuthnRequests og Nemlog-in's konfiguration.

Udseendet af AuthnRequests kan variere fra løsning til løsning afhængigt af den anvendte SAML teknologi samt hvordan SAML teknologien konkret er konfigureret.

3.1 Er <AuthnRequest> korrekt signeret?

Dette en af de mest almindelige forekommende fejl, hvor AuthnRequest er signeret med et certifikat der ikke kan accepteres af Nemlog-in.

Årsagen til dette kan skyldes en række forskellige forhold. Der henvises til afsnittet "2.1 Benytter jeg det korrekte signeringscertifikat" for detaljeret gennemgang.

3.2 Er NameIDPolicy angivet i <AuthnRequest>?

Undgå at angive NameIDPolicy i AuthnRequest. NameIDPolicy er konfigureret for din løsning i Nemlog-in gennem udveksling af metadata. AuthnRequests kan derfor blive afvist, særligt hvis der er konflikt med konfigurationen eller hvis NameIDPolicy ikke er blandt de understøttede formater, som er "Persistent" og "X509SubjectName".

Eksempel på AuthnRequest med NameIDPolicy der vil fejle:

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="_fec36d8804357a72394d049499cad23aff59199ce0"
Version="2.0" IssueInstant="2012-01-23T10:24:09Z" Destination="https://login.test-nemlog-
in.dk/adfs/ls/" IsPassive="false" AssertionConsumerServiceIndex="0">
  <saml:Issuer>https://sp1.test-nemlog-in.dk</saml:Issuer>
<samlp:NameIDPolicy AllowCreate="false" Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress"></samlp:NameIDPolicy>
</samlp:AuthnRequest>
```

3.3 Er Assertion Consumer Service korrekt angivet I <AuthnRequest>?

Der er flere måder at erklære det endpoint, hvortil din løsning modtager <response> meddelelse fra Nemlog-in.

Det anbefales at erklære attributten AssertionConsumerServiceIndex der instruerer Nemlog-in til at anvende den konfigurerede <response> lokation for din løsning inklusive den konfigurerede protokolbinding. Alternativt kan attributten AssertionConsumerServiceUrl sammen med attributten ProtocolBinding erklæres, som instruerer Nemlog-in til at anvende de medsendte attributter og ignorere de konfigurerede værdier for din løsning.

Bemærk i øvrigt:

- Hvis attributterne kombineres på andre måder, vil det formodentligt få Nemlog-in til at afvise din AuthnRequest.
- Hvis ingen attributter angives vil Nemlog-in defaulte til de konfigurerede værdier.

Eksempel på AuthnRequest med AssertionConsumerServiceIndex:

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="_fec36d8804357a72394d049499cad23aff59199ce0"
Version="2.0" IssueInstant="2012-01-23T10:24:09Z" Destination="https://login.test-nemlog-
in.dk/adfs/ls/" IsPassive="false" AssertionConsumerServiceIndex="0">
  <saml:Issuer>https://sp1.test-nemlog-in.dk </saml:Issuer>
</samlp:AuthnRequest>
```

Eksempel på AuthnRequest med AssertionConsumerServiceUrl og ProtocolBinding:

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="_fec36d8804357a72394d049499cad23aff59199ce0"
Version="2.0" IssueInstant="2012-01-23T10:24:09Z" Destination="https://login.test-nemlog-
in.dk/adfs/ls/" IsPassive="false" AssertionConsumerServiceUrl=https://sp1.test-nemlog-
in.dk/SAML20/login ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST">
  <saml:Issuer>https://sp1.test-nemlog-in.dk</saml:Issuer>
</samlp:AuthnRequest>
```

3.4 <Scoping> element i <AuthnRequest>

Undgå at erklære <Scoping> elementet i <AuthnRequest>, i det Nemlog-in ikke understøtter denne, og derfor vil fejle under login.

Dette bør kun påvirke proxy Identity Providers, hvor der i OIOSAML Web SSO [2] findes reference til <Scoping> elementets anvendelse.

3.5 <RequestedAuthnContenxt> element i <AuthnRequest>

Undgå at erklære <RequestedAuthnContext> elementet i <AuthnRequest>, i det Nemlog-in ikke understøtter denne, og derfor vil fejle under login.

Bemærk, at der i en tidligere version af OIOSAML Web SSO [2] fandtes en reference til anvendelse af dette element, som ikke længere er gældende.

4 Min løsning fejler efter login i Nemlog-in

Efter Nemlog-in har behandlet AuthnRequest sender Nemlog-in et <response> til din løsning indeholdende en Assertion.

Dette afsnit beskriver mulige scenarier, som kan forårsage at din løsning fejler efter modtagelse af assertion fra Nemlog-in. Det skal understreges, at i Nemlog-in's optik er login gennemført med succes og fejlsøgning skal derfor ske lokalt i din løsning.

4.1 Min løsning kan ikke dekryptere assertion

NemLog-in benytter sig af krypteringsmetoderne "AES-256" til block encryption og "RSA-OAEP" til key transport. Din løsning skal ligeledes understøtte disse for at kunne dekryptere assertion.

Bemærk, at Nemlog-in1 benytter "AES-128" samt "RSA-1.5".

4.1.1 Java Cryptography Extension (JCE)

Hvis du benytter OIOSAM.JAVA referenceimplementeringen eller anden Java baseret SAML klient, skal "JCE Unlimited Strength Jurisdiction Policy Files v6" være installeret for understøttelse af "AES-256".

JCE kan hentes her: http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html

4.2 Min løsning forventer type-erklæring i <AttributeValue> elementer

Nemlog-in erklærer kun type i <AttributeValue> elementer såfremt at typen er forskellig fra "xs:string". Din løsning skal derfor betragte "xs:string" som default-type for <AttributeValue> elementer.

Ovenstående adfærd adskiller sig fra Nemlog-in1, hvor type (antageligt) altid erklæres eksplicit. På baggrund af gennemførte tests er det NNIT's vurdering, at de færreste løsninger vil opleve problemer med adfærden.

5 Referencer

[1] Bekrivelse af migreringstestmiljø.
[2] OIOSAML Profile version 2.0.8 på digitaliser.dk.

6 Ændringslog

Dato	Version	Beskrivelse	Initials
10.02.2012	0.a	Dokument oprettet	MWL
21.02.2012	1.0	Endelig version	MWL
24.02.2012	1.0	Godkendt	SQWI
09.03.2012	1.0	Opdateret afsnittet vedr. NameIDFormat, som skal angives i metadata. Dokument godkendt.	MWL
07.05.2012	2.0	Opdateret introduktionsafsnit med ændringer til entityId og URL'er til login/logout bindinger.	MWL
12.12.2012	2.a	Opdateret indhold i forbindelse med release a go-live: • I afsnit "Introduktion" er oplysning om ændring til entity ID blevet fjernet. • 3.4 + 3.5 tilføjet.	MWL
13.12.2012	2.a	Reviewet og kommenteret.	NiNN/ JBHQ
13.12.2012	3.0	Kommentarer indarbejdet og dokument godkendt	MWL