

Test af udfasning af OCES attributter

15. februar 2021

Trin-for-trin guide

Som varslet i nyheder og webinarer udfases en række attributter i NemLog-in per 14/6 - 2021. Denne guide forklarer trin-for-trin, hvordan tjenesteudbydere kan teste, hvorledes deres it-systemer reagerer, når attributterne ikke længere leveres af NemLog-in.

Udfasede attributter

Nedenstående attributter vil ikke længere blive leveret i SAML billetter fra NemLog-in, uanset om brugeren logger ind med NemID eller MitID fremadrettet:

- UserCertificate (urn:oid:1.3.6.1.4.1.1466.115.121.1.8)
- Certificate issuer (urn:oid:2.5.29.29)
- (Certificate) serial number (urn:oid:2.5.4.5)
- IsYouthCert (dk:gov:saml:attribute:IsYouthCert)
- UniqueAccountKey (dk:gov:saml:attribute:UniqueAccountKey)
- Postal address (urn:oid:2.5.4.16)
- Title (urn:oid:2.5.4.12)
- Organization unit (urn:oid:2.5.4.11)
- UserAdministratorIndicator (dk:gov:saml:attribute:UserAdministratorIndicator)

Forberedelse af test

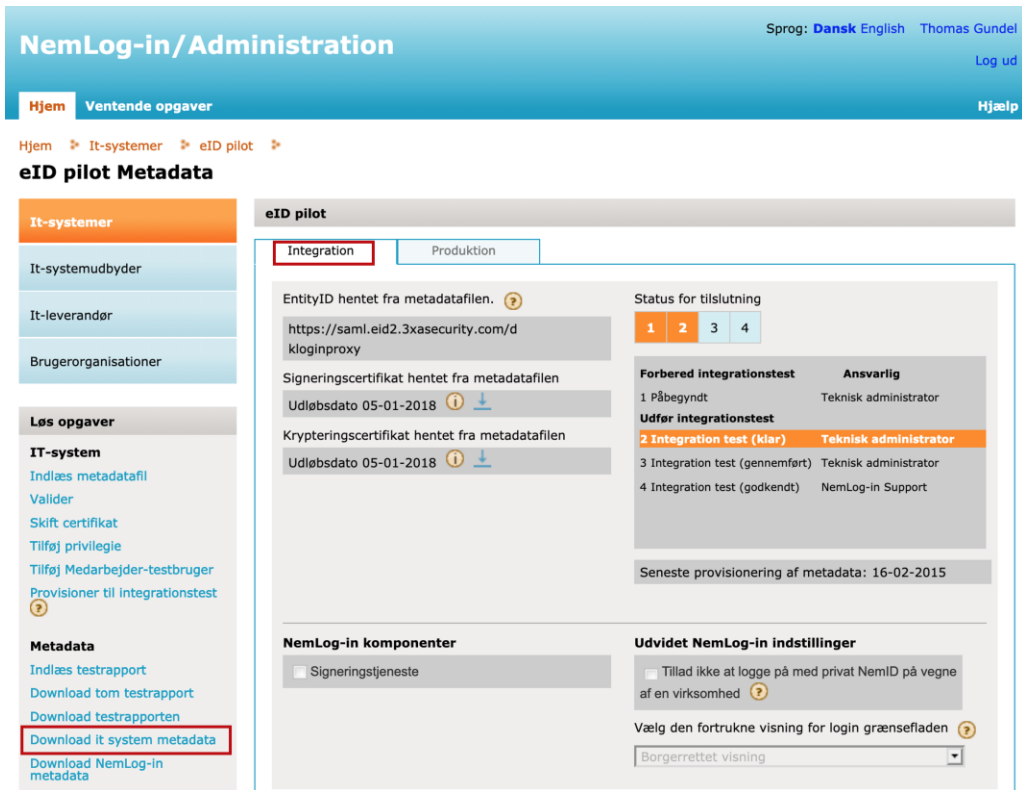
Som tjenesteudbydere kan I teste påvirkningen af jeres it-systemer ved brug af NemLog-in's integrationstestmiljø. Hvis I endnu ikke har en fungerende integration mellem jeres eget testmiljø og NemLog-in's integrationstestmiljø, skal en sådan først etableres, før I kan teste.

I kan forberede testen ved at fjerne de nævnte attributter fra metadatafilen og genuploade samt provisionere denne til NemLog-in's integrationstestmiljø. Herefter vil attributterne ikke længere optræde i de SAML Assertions som NemLog-in udsteder ved brugerautentifikation mod it-systemet.

Forbered testen ved at udføre følgende trin:

1. Log på NemLog-in's administrationsportal ved brug af et OCES medarbejdercertifikat, der er oprettet som teknisk administrator for det it-system, der skal testes. Adressen er: <https://administration.nemlog-in.dk>
2. Lokalisér og klik på systemet i oversigten it-systemet for at se detaljer.
3. Sørg for at vælge fanen "Integration".

Et skærbillede som nedenstående fremkommer:



The screenshot shows the NemLog-in/Administration interface. The top navigation bar includes 'Hjem', 'Ventende opgaver', and 'Hjælp'. The main content area is titled 'eID pilot Metadata'. On the left, there is a sidebar with 'It-systemer' and 'Løs opgaver' sections. The 'Løs opgaver' section has a sub-section 'IT-system' with several links, including 'Download it system metadata' which is highlighted with a red box. The main content area has a tabbed interface with 'Integration' and 'Produktion' tabs. The 'Integration' tab is active, showing a list of integration tests. The 'Integration test (klar)' row is highlighted with a red box. Below the list, there is a section 'NemLog-in komponenter' with a checkbox for 'Signeringstjeneste'. At the bottom, there is a section 'Udvidet NemLog-in indstillinger' with a checkbox for 'Tillad ikke at logge på med privat NemID på vegne af en virksomhed' and a dropdown menu for 'Vælg den fortrukne visning for login grænsefladen'.

4. Klik på menuen i venstre side med titlen "Download it system metadata" markeret med rødt på figuren ovenfor.
5. Gem filen og tag en sikkerhedskopi.
6. Åben filen med en editor, som er velegnet til at redigere XML filer og find blokken `<md:AttributeConsumingService>`
7. Gennemgå omhyggeligt listen med attributter og fjern eller udkommentér alle attributter, som udfases (jævnfør ovenstående liste).

Eksempel hvor de røde pile angiver linjer, der skal slettes:

```
<md:AttributeConsumingService index="0" isDefault="true">
  <md:ServiceName xmlns:xml="http://www.w3.org/XML/1998/namespace" xml:lang="en">https://eid2.3xasecurity.com/dkloginproxy</md:ServiceName>
  <md:RequestedAttribute Name="urn:oid:2.5.4.4" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
  <md:RequestedAttribute Name="urn:oid:0.9.2342.19200300.100.1.1" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
  <md:RequestedAttribute Name="urn:oid:0.9.2342.19200300.100.1.3" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
  <md:RequestedAttribute Name="dk:gov:saml:attribute:AssuranceLevel" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
  <md:RequestedAttribute Name="dk:gov:saml:attribute:SpecVer" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
  <md:RequestedAttribute Name="urn:oid:2.5.4.5" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
  <md:RequestedAttribute Name="dk:gov:saml:attribute:IsYouthCert" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
  <md:RequestedAttribute Name="urn:oid:2.5.29.29" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="true" />
  <md:RequestedAttribute Name="dk:gov:saml:attribute:UniqueAccountKey" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="false" />
  <md:RequestedAttribute Name="urn:oid:2.5.4.10" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="false" />
  <md:RequestedAttribute Name="urn:oid:2.5.4.11" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="false" />
  <md:RequestedAttribute Name="urn:oid:2.5.4.12" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="false" />
  <md:RequestedAttribute Name="urn:oid:2.5.4.16" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="false" />
  <md:RequestedAttribute Name="urn:oid:2.5.4.65" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="false" />
  <md:RequestedAttribute Name="urn:oid:1.3.6.1.4.1.1466.115.121.1.8" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="false" />
  <md:RequestedAttribute Name="dk:gov:saml:attribute:PidNumberIdentifier" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="false" />
  <md:RequestedAttribute Name="dk:gov:saml:attribute:CprNumberIdentifier" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="false" />
  <md:RequestedAttribute Name="dk:gov:saml:attribute:IdNumberIdentifier" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="false" />
  <md:RequestedAttribute Name="dk:gov:saml:attribute:Privileges_intermediate" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" isRequired="false" />
</md:AttributeConsumingService>
```

8. Gem den modificerede metadatafil.
9. I administrationsportalen vælges ”Indlæs metadatafil” i menuen til venstre.



10. Vælg herefter den opdaterede fil i dialogen og tryk ”Indlæs metadatafil”.
11. Herefter fremkommer en i dialog i stil med nedenstående:

NemLog-in/AdministrationSprog: Dansk English Thomas Gundel
Log ud

Hjem Ventende opgaver Hjælp

Upload og validering metadata gennemført
[Gå tilbage til Rediger tekniske oplysninger >](#)

Luk

Hjem » It-systemer » eID pilot » eID pilot metadata »

Indlæs metadatafil

Metadatafil
Vælg den metadatafil (XML-format), som du ønsker at indlæse fra din computer. Filen vil automatisk blive valideret af metadatavalidatoren inden indlæsning.
 Ingen fil valgt.

< Tilbage Indlæs metadatafil

12. Kontroller via status i den ”gule boks” om indlæsningen gik godt og ret evt. yderligere fejl i metadatafilen.
13. Tryk på ”<Tilbage” knappen og kontroller om listen af attributter i bunden af skærbilledet nu er korrekt opdateret, så de udfasede attributter ikke længere fremgår af listen:

Avanceret

Attributter	Privilegier	Endpoints	Testbrugere	Delte privil...
It-systemet har følgende attributter				
Attributnavn ▲	Attributter			
	urn:oid:2.5.4.4			
	urn:oid:2.5.4.3			
	urn:oid:0.9.2342.19200300.100.1.1			
	urn:oid:0.9.2342.19200300.100.1.3			
	dk:gov:saml:attribute:AssuranceLevel			
	dk:gov:saml:attribute:SpecVer			
	dk:gov:saml:attribute:CvrNumberIdentifier			
	urn:oid:2.5.4.10			
	urn:oid:2.5.4.65			
	dk:gov:saml:attribute:PidNumberIdentifier			
	dk:gov:saml:attribute:CprNumberIdentifier			
	dk:gov:saml:attribute:RidNumberIdentifier			
	dk:gov:saml:attribute:Privileges_intermediate			

14. Vælg nu menuen ”Provisioner til integrationstest” til venstre.
15. Tryk herefter på knappen ”Anmod om integrationstest” og verificér, om upload gik godt, eller om der er fejl i metadatafilen (markeret i den gule boks). Det kan fx være, at certifikatet¹ i metadatafilen er udløbet siden sidste gang metadata blev uploadet - og derfor skal udskiftes. I givet fald skal man både huske at udskifte certifikat i metadatafil og på servere i eget testmiljø, som skal kalde NemLog-in med samme certifikat, som er angivet i metadatafilen.

¹ Der er tale om et FOCES/VOCES testcertifikat.

Bemærk, at metadata ikke kan ændres før integrationstest har været gennemført

Anmod om integrationstest

Nedenfor ses skærmbillede efter succesfuld provisionering af nye metadata til integrationstestmiljø (læg mærke til de røde bokse med markeringer): dels angiver status i den gule statuslinje, at provisionering er gennemført, dels angiver den orange statusindikator, at der kan udføres integrationstest, og endelig angiver dato for seneste provisionering, at der er overført nye metadata:

NemLog-in/Administration

Sprog: Dansk English Thomas Gundel
Log ud Hjælp

Hjem Ventende opgaver

Du har nu anmodet om at foretage integrations test af eID pilot. Du vil nu modtage en besked og en ny opgave under 'Mine opgaver' der skal benyttes i det videre forløb.

Luk

Hjem » It-systemer » eID pilot »
eID pilot Metadata

It-systemer

It-systemudbyder

It-leverandør

Brugerorganisationer

Løs opgaver

IT-system

Indlæs metadatafil

Valider

Skift certifikat

Tilføj privilegie

Tilføj Medarbejder-testbruger

Provisioner til integrationstest

Metadata

Indlæs testrapport

Download tom testrapport

Download testrapporten

Download it system metadata

Download NemLog-in metadata

eID pilot

Integration Produktion

EntityID hentet fra metadatafilen.
https://saml.eid2.3xasecurity.com/d/loginproxy
Signeringscertifikat hentet fra metadatafilen
Udløbsdato 16-12-2022
Krypteringscertifikat hentet fra metadatafilen
Udløbsdato 16-12-2022

Status for tilslutning
1 Påbegyndt 2 Udfør integrationstest 3 Integration test (gennemført) 4 Integration test (godkendt)
Forbered integrationstest Ansvarlig
1 Påbegyndt Teknisk administrator
2 Udfør integrationstest
2 Integration test (klar) Teknisk administrator
3 Integration test (gennemført) Teknisk administrator
4 Integration test (godkendt) NemLog-in Support
Seneste provisionering af metadata: 05-01-2021

NemLog-in komponenter
☐ Signeringsjeneste

Udvidet NemLog-in indstillinger
☐ Tillad ikke at logge på med privat NemID på vejne af en virksomhed
Vælg den fortrukne visning for login grænsefladen
Borgerrettet visning