



DIGITALISERINGSSTYRELSEN

Spørgetime

NemLog-ins nye testmiljø: Test OIOSAML 3, ny
signeringsløsning og nye oplagstjenester.

28. april 2021 – klokken 10.00-11.00





Christian Schmidt-
Madsen
It-arkitekt,
Digitaliseringsstyrelsen



Thomas Gundel
Ekstern konsulent,
Digitaliseringsstyrelsen



Thomas Mostrup
Nymand
Løsningsarkitekt,
Nets

Dagsorden

- Besvarelse af indkomne spørgsmål
- Åben Q&A





Indkomne spørgsmål



DIGITALISERINGSSTYRELSEN

Indkomne spørgsmål

1. Hvornår åbnes der for, at borgere kan benytte MitID via NemLog-in?

- Det nye NemLog-in går i luften med NemLog-in broker den 14. juni 2021. Tjenesteudbydere, som er tilsluttet NemLog-in, kan derefter tilbyde deres brugere at logge ind med NemID og MitID.
- Se slide 8 med tidslinje.



Indkomne spørgsmål

2. Ift. Go-live på MitID den 6. maj 2021, er det korrekt forstået, at hvis ikke man bruger andre brokere end NemLog-in, så skal man som myndighed ikke foretage nogle ændringer? Altså at opgaven udelukkende ligger hos Digitaliseringsstyrelsen og Nets DanID?

- Der sker ingen ændringer i NemLog-in den 6. maj. NemLog-ins nye broker har go-live den 14. juni. Herefter kan borgere logge på med både MitID og NemID, både hos TU, der er tilsluttet OIOSAML 2.1.0 og OIOSAML 3.
- Alle TU skal dog i løbet af migreringsperioden frem til december 2021 migrere til OIOSAML 3 snitfladen og evt. tage ny signeringsløsning i brug.
- Se slide 8 med tidslinje.



Indkomne spørgsmål

3. *Hvornår forventes det, at der bliver lukket for NemID?*

- NemID vil fungere parallelt med MitID i en længere overgangsperiode, indtil migreringen af hhv. borgere og virksomheder er gennemført.
- Se slide 8 med tidslinje.



2021

2022

Q2

Q3

Q4

Q1

NemLog-in

NemLog-in

Ny NemLog-in Broker (Log-in)



Pilot

14. juni: Go-live Broker



Go-live Signering



6. dec.: Go-live MitID Erhverv

MitID



Pilot

6. maj: Go-live MitID

Borgere
Medarbejdere

Log-in med NemID

Log-in med MitID og NemID

Log-in med NemID medarbejdersignatur

Log-in med MitID Erhverv og NemID

Tjenesteudbydere

22. april Beta-testmiljø OIOSAML 2.1.0 og 3

Beta-testmiljø

Int

Pilot

Migrering

Teknisk snitflade

OIOSAML 2.0.9

OIOSAML 2.1.0

OIOSAML 3



Indkomne spørgsmål

4. Jeg går ud fra, at produktion i dag er med WebSSO 2.0.9. Kommer WebSSO 2.1.0 på test før den kommer på produktion, og hvornår sker disse to ting?

- OIOSAML 2.1.0 er aktivt pt. på beta-testmiljøet. Der er desuden udgivet vejledning til at afprøve sin integration uden de OCES-attributter, som udfases med 2.1.0.
- [Hent guiden her](#), eller find den på NemLog-in portalen.
- 2.1.0 vil desuden komme i integrationstestmiljøet forud for idriftsættelsen i produktion.



Indkomne spørgsmål

5. Skal OIOSAML3.java anvendes fremfor version 2.2.1 til NemLog-in version 3? Og giver det mening at migrere til OIOSAML2 nu, for derefter at opgradere til OIOSAML3, når den går i luften?

- Vi anbefaler generelt, at den seneste version af referenceimplementeringer ibrugtages hurtigst muligt. Både i forhold til kompatibilitet og sikkerhed.
- Hvis man er ny TU på NemLog-in, skal man tilslutte sig OIOSAML 3, som kan afprøves i beta-testmiljøet nu.



Indkomne spørgsmål

6. Kan OIOSAML3.java udvides med en klasse i applikationen til håndtering af login, som i version 2.2.1?

- Vi har noteret ønsket i backlog.



Indkomne spørgsmål

7. Er det med OIOSAML3.java nødvendigt, at applikationen tjekker NSIS_LOA/ AssuranceLevel efter login - eller sikrer OIOSAML3.java dette?

- Nej, hvis I anvender AssertionValidatorService og AuthenticatedFilter fra OIOSAML3.Java, foretages den nødvendige kontrol af NSIS LoA/Assurance Level jf. den konfiguration, I har angivet.



Indkomne spørgsmål

8. Kan vi få gennemgået retningslinjer for log-in flowet for mobile apps?

- Mobile apps bør foretage log-ins med systembrowseren efter samme mønster, som findes i OAuth og OpenID Connect.
- Der bør ikke benyttes webviews, men systembrowseren. Dels af hensyn til sikkerhed og dels i forhold til transparens for brugeren. De bør kunne se, hvor de logger ind.



Indkomne spørgsmål

9. *Kommer der referenceeksempler for en matchservice?*

- Det er der ikke planer om på nuværende tidspunkt.



Indkomne spørgsmål

10. Vil den nuværende NemLog-in platform (OIOSAML 2) også komme til at understøtte MitID, eller bliver det kun tilgængeligt via OIOSAML 3?

- Begge IdP'er (2.0.9 og 3.0.2) kan autentificere brugere med både NemID og MitID - jævnfør gennemgang på webinarret den 23. marts om "bro i migreringsperioden".



Indkomne spørgsmål

11. Vedr. testdata CPR-nr.: På webinar 23. marts fortalte I, at testmedarbejderen skal have CPR-nr. for at kunne blive tilknyttet testvirksomheden. I FOTM har I testmedarbejder med CPR-nr. Har I også oprettet det til NemLog-in 3? Eller ved I, hvordan vi kan få testdata med CPR-nr., så vi kan undgå at bruge virkelige CPR-nr.

- Når I opretter testbrugere i beta-testmiljøet, kan I angive fiktive CPR-numre i vores MitID simulator.
- Det er ikke tilladt at anvende rigtige CPR-numre i testmiljøerne!



Indkomne spørgsmål

12. *Forventes OIOSAML 2.0.9 attributterne fortsat udfaset den 14. juni 2021?*

- Ja.



Indkomne spørgsmål

13. Vi ved, at I ikke har en præcis dato for, hvornår IdP 2.1.0 udgår, så der kun er IdP 3 kørende fremover. Men kunne I give et meget groft estimat, plus/minus 3 måneder, for, hvornår det sker, at IdP 2.1.0 udfases?

- Migrering inden december 2021 er målet. Der kan dispenseres ved fx tjenester, der udgår inden for kort tid eller erstattes af ny tjeneste. Der er ikke truffet beslutning om endelig nedlukning.



Indkomne spørgsmål

14. Er det korrekt forstået, at man skal supportere både den nuværende og nye signeringsløsning i en overgangsperiode, for at være sikker på, at ens brugere kan signere med både NemID og MitID? Og hvordan sikrer man, at man får brugerne over på den rigtige signeringsløsning?

- Ja, NemID signeringer udføres med den gamle signeringstjeneste, og MitID signeringer med den nye.
- Vi anbefaler, at alle, der bruger signering, skifter til OIOSAML 3.0.2 til autentifikation, hvor man i SAML Assertion kan få en indikation af, hvordan brugeren er logget ind. NSIS sikringsniveau returneres for MitID autentifikationer, og den gamle OIOSAML 2.0.9 Assurance Level attribut returneres for NemID autentifikationer. Alternativt kan man lave to knapper i brugerfladen: "signér med NemID" og "signér med MitID".



Indkomne spørgsmål

15. *Hvordan styrer man, hvilken version af OIOSAML man kobler op imod?*



- Det styres i administrationsportalen, hvor tilslutning til OIOSAML 2.1.0 og 3.0.2 er to forskellige indgange.
- Tjenester, der i dag er tilsluttet 2.0.9, skal ikke gøre noget for at komme på 2.1.0 (endpoint opgraderes automatisk), så det er kun ved tilslutning til 3.0.2, at man aktivt skal gøre noget som tjenesteudbyder.

Indkomne spørgsmål

16. Vi står over for at skulle migrere fra en ren NemID implementering til NemLog-in, for at understøtte MitID, når det går i luften. Hvilken OIOSAML snitflade skal vi benytte?

- Alle tjenesteudbydere, der ønsker at integrere til NemLog-in, skal anvende OIOSAML 3 profilen.



Indkomne spørgsmål

17. Er det korrekt forstået, at der fremover, når PID er endeligt udfaset, ikke findes en opslagstjeneste, hvor man kan hente en privatbrugers CPR-nr., eller en tjeneste, hvor man kan verificere et CPR-nr. indtastet af brugeren?

- Når NemID udfases, forventer vi at migrere PID-CPR data fra NemID-løsningen ind i NemLog-in. Herefter vil DIGST kunne understøtte opslag i en efterfølgende periode.
- Med en kommende NemLog-in leverance leverer Nets en tjeneste, der erstatter NemID PID-CPR match. Denne tjeneste vil også være tilgængelig, efter NemID er udfaset.



Indkomne spørgsmål

18. Vil PID/RID-attributterne indgå i SAML-token for brugere, der logger på uden brug af certifikat (fx MitID)?

Eller modtager tjenesten i dette tilfælde kun oplysning om UUID for brugere, og skal dermed i praksis være i stand til at håndtere dette scenarie fra den 14. juni 2021?

- Ja, PID/RID vil - i en lang overgangsperiode - indgå i SAML-token også for brugere, der logger på med MitID. Denne egenskab er grundlag for den anbefalede dynamiske migreringsstrategi for brugerkonti, som vi gennemgik på forrige webinar.



Indkomne spørgsmål

19. Vi har systemer, der bruger PID og RID funktionelt. Hvor længe kan vi forsætte med det, før det udgår helt?

- Som minimum resten af 2021.



Indkomne spørgsmål

20. Er det muligt at fastsætte forskellige sikringsniveauer for hhv. private og erhvervsidentiteter, der logger på NemLog-in – fx så en privatperson kan logge på med niveau "Lav", mens en erhvervsbruger bliver mødt med krav om "Betydelig"?

- Ja, men det gør I i jeres tjeneste, i forbindelse med behandling af autentifikationssvaret fra NemLog-in. Man kan ikke forespørge på kombinationen af person/Lav og medarbejder/Betydelig i autentifikationsanmodningen.



Indkomne spørgsmål

21. Vil signeringssvaret indeholde CPR-nr., eller vil det være nødvendigt efterfølgende at bruge en af opslagstjenesterne for at få CPR-nr.?

- Signeringssvar indeholder aldrig CPR-nummer, men i stedet et certifikat, med en UUID-baseret identifier. Denne UUID kan man så arbejde videre med i opslags- eller matchtjenester.
- Hvis man har fået CPR i SAML Assertion ifm. Log-in, kan man se, om UUID i signeringssvar matcher Subject i Assertion (metoden SubjectMatchesSigner).



Indkomne spørgsmål

22. *Hvornår kan vi udstede system- og organisationscertifikater til vores eget CVR, som ikke kan revokes af nogen, der kan gætte username + password til selvbetjeningen?*

- Vi anbefaler, at man anvender et stærkt password, som overholder gængse retningslinjer for stærke passwords. Der er desuden mulighed for at nulstille sit password i MitID simulatoren.



Indkomne spørgsmål

23. *Er der nogen løsning endnu til at afgøre, om en person er medarbejder i en virksomhed med et bestemt CVR-nummer?*

- Der er nogle særlige tjenester til brokere, som gør dette muligt. Eksempelvis kan brokern på baggrund af et MitID autentifikationssvar se, om der findes erhvervsidentiteter tilknyttet brugeren i NemLog-in. Men som sagt: disse tjenester er forbeholdt NSIS-anmeldte brokere.



Indkomne spørgsmål

24. Kommer der noget udviklerrettet dokumentation, der beskriver, hvordan metadata-filerne skal sættes op? Denne information har været meget svær at finde tidligere.

- Der står krav til metadata i OIOSAML 3.0.2 profilen, og på vejledningssiderne har vi nu uploadet et eksempel.
- Desuden findes info om integration generelt på vejledningssiderne:
www.nemlog-in.dk/vejledningertiltestmiljo/



Indkomne spørgsmål

25. *Hvornår kan man anses for at være en offentlig tjenesteudbyder?*

- Offentlige myndigheder og offentligretlige organer, som anvender en digital selvbetjeningsløsning til at udføre en myndighedsopgave, skal anvende dele af NemLog-in, hvis adgangen til den digitale selvbetjeningsløsning kræver sikker autentifikation.





Åben Q&A



DIGITALISERINGSSTYRELSEN

Links til hjemmesider, vejledninger og dokumentation

- Se og læs mere på den nye NemLog-in portal: www.nemlog-in.dk
- Tilmeld dig NemLog-in nyhedsbrev og få nyheder samt løbende information om det nye NemLog-in, der er relevant for dig og din virksomhed/myndighed. [Tilmelding via NemLog-in portalen](#).
- Se og læs mere på vores NemLog-in og MitID implementeringssite: www.digst.dk/it-loesninger/implementeringssite
- Læs mere om det nye NemLog-in: <https://migrering.nemlog-in.dk/om-nemlog-in/>
- Læs mere om NSIS: <https://migrering.nemlog-in.dk/nemlog-in-broker/offentlig-tjenesteudbyder/nsis/>
- Læs mere om OIO SAML standarden: <https://migrering.nemlog-in.dk/nemlog-in-broker/offentlig-tjenesteudbyder/oiosaml-3-0-2/>
- Test af udfasning af OCES attributter: <https://migrering.nemlog-in.dk/media/8d8b3d6a971357d/trin-for-trin-guide-test-af-udfasning-af-oces-attributter.pdf>
- Læs mere om de nye certifikatpolitikker: <https://migrering.nemlog-in.dk/nemlog-in-broker/offentlig-tjenesteudbyder/certifikater/>
- Se tidligere afholdte webinarer og infovideoer om NSIS, Lokal IdP og OIOSAML: <https://migrering.nemlog-in.dk/kontakt-og-support/infovideoer-og-webinarer/>

Tak for i dag



Christian Schmidt-
Madsen
It-arkitekt,
Digitaliseringsstyrelsen



Thomas Gundel
Ekstern konsulent,
Digitaliseringsstyrelsen



Thomas Mostrup
Nymand
Løsningsarkitekt,
Nets