DIGITALISERINGSSTYRELSEN

Bilag A

27. september 2018

Til høringsparterne
Se vedlagte liste (*Bilag B*)

DIGITALISERINGSSTYRELSEN

Høring i forbindelse med opdatering af OIOSAML 3.0 profilen

Digitaliseringsstyrelsen har opdateret vedlagte OIOSAML profil forud for udvikling af NemLog-in3 løsningen. Høringen er sendt til de myndigheder og organisationer m.v., der fremgår af vedlagte høringsliste.

Høringsbrev (*Bilag A*), høringsliste (*Bilag B*), svarskabelon (*Bilag C*) og profil (*Bilag D*) er også tilgængelige på høringsportalen.

Baggrund

Den nuværende OIOSAML 2.0.9 profil fra 2012 benyttes bl.a. i forbindelse med fødereret log-in og single sign-on (SSO) til offentlige selvbetjeningsløsninger herunder portalerne Borger.dk og Virk.dk. Profilen har til formål at sikre interoperabilitet i implementeringen af SAML2 standarden, og er blandt andet implementeret af NemLog-in2 og de mere end 300 myndighedsløsninger, som er tilsluttet NemLog-in-føderationen.

I næste generation af den fællesoffentlige infrastruktur til håndtering digitale identiteter sker der en række ændringer, som medfører behov for opdatering af OIOSAML profilen.

De væsentligste bevæggrunde for modernisering af profilen har været:

- Den kommende fællesoffentlige identitetsinfrastruktur (MitID og NemLog-in3) kommer til at adskille eID fra eSignatur, og OCES-infrastrukturen vil blive redesignet.
- Generelt vil OCES-specifikke attributter blive fjernet fra profilen, og der overgås til mere teknologineutrale og fremtidssikre identifiers baseret på UUID'er.
- En række nye forretningsbehov er identificeret under foranalyserne forud for kravspecificeringen af den nye infrastruktur.
- Indførelsen af ny databeskyttelsesregulering (GDPR og Databeskyttelsesloven) og det øgede fokus på privacy har medført et behov for omstrukturering af profilen, således at der opnås privacy-by-design og privacy-by-default. Eksempelvis er identifiers i udgangspunktet specifikke for den enkelte tjenesteudbyder, så brugerens transaktioner ikke kan kobles på tværs af tjenesteudbydere. Tjenesteudbydere, der har lovhjemmel og behov for at få persistente identifiers som fx CPR-numre, kan dog fortsætte med dette.
- Introduktion af muligheden for private tjenesteudbydere på NemLog-in3 kræver ligeledes en række tilpasninger.
- Indførelsen af National Standard for Identiteters Sikringsniveauer (NSIS) har medført behov for at tilpasse håndtering af sikringsniveauer (LoA) i profilen.
- Der er et generelt behov for at opdatere kryptografiske algoritmer og nøglelængder til et tidssvarende niveau.

OIOSAML 3.0 er beskrevet som en ren 'to-be' profil, som på sigt vil erstatte OIOSAML 2.0.9. Eksempelvis forventes NemLog-in3 at benytte OIOSAML 3.0 som sin primære snitflade, når den går i drift i 2020. Der kan i en overgangsperiode være behov for at understøtte både ny og gammel profil eller evt. hybrider – men der endnu ikke foretaget en detaljeret planlægning af overgangsforløbet. Der foreligger endvidere heller ikke nogen dato for, hvornår tjenesteudbydere forventes at have skiftet til den nye profil. Den tidlige høring og udarbejdelse af profil vil imidlertid give tjenesteudbyderne en lang periode til at tilpasse deres implementeringer, inden den nye identitetsinfrastruktur går i drift.

Digitaliseringsstyrelsen planlægger efter høringen at udarbejde en separat vejledning til OIOSAML 3.0 med yderligere forklaringer og eksempler.

De vigtigste ændringer i OIOSAML 3.0

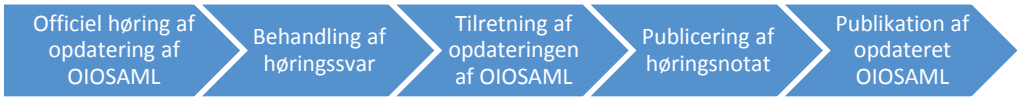
Nedenfor er oplistet de vigtigste ændringer i OIOSAML 3.0 – der er dog flere ændringer i profilen, så høringsparterne opfordres til at gennemgå den nye version i detaljer:

- Profilen har fået en ny struktur med udgangspunkt i SAML2Int profilen fra Kantara Initiative. Herved er fokus på de normative krav fremhævet, så det bliver lettere at vurdere og teste om en implementering lever op til kravene. Yderligere forklaringer og eksempler udgives som tidligere nævnt i en separat vejledning til profilen, så krav adskilles fra forklaringer.
- Der er defineret to nye attributprofiler for hhv. personer og professionelle (OCES-specifikke attributter udgår), RID og PID fortsætter med status som deprekerede.
- Identifiers er baseret på UUID'er og Subject feltet bærer altid en tjenesteudbyderspecifik identifier.
- Krav til kryptografiske algoritmer og nøglelængder er skærpet.
- Håndtering af 'levels of assurance' sker i henhold til NSIS, og der er indført mulighed for at angive et ønsket sikringsniveau i forespørgsler fra tjenesteudbydere (herunder muligheden for step-up autentifikation).
- Der er indført krav om support for multiple certifikater i metadatafiler.
- Det er nu tilladt at anvende et kvalificeret certifikat for en juridisk person i metadata.

Bemærk, at ovenstående ikke er en udtømmende liste over ændringer og således blot kan opfattes som udvalgte eksempler.

Videre proces

Opdateringen af OIOSAML forventes publiceret medio januar 2019, og den følgende proces er illustreret i nedenstående figur 1.



Figur 1 – illustration af den følgende proces indtil publicering af opdateringen af standarden.

Interessenter og høringsparter opfordres til at afgive kommentarer og supplerende oplysninger, som findes relevante for OIOSAML. Kommentarer og supplerende oplysninger bedes indsat i vedlagt svarskabelon (se *Bilag C*).

Det skal understreges, at kravene i opdateringen af OIOSAML og den tilhørende vejledning er foreløbige og kan blive ændret som følge af høringssvarene.

Digitaliseringsstyrelsen vil efter modtagelse af høringssvar udarbejde høringsnotat samt eventuelle tilretninger til profilen.

Digitaliseringsstyrelsen anmoder om, at bemærkninger sendes til saslh@digst.dk. Eventuelle spørgsmål vedrørende standarden sendes til Sandra Schöne Leth Hansen saslh@digst.dk. Høringssvar skal være Digitaliseringsstyrelsen i hænde **senest fredag den 14.12.2018.**