Digitaliserings-
styrelsen

Høringsnotat

30. januar 2025

Behandling af indkomne høringssvar i forbindelse med høring om OIOSAML 4

Om høringen

Udkastet til OIOSAML 4 profilen har fra den 4. november 2024 til den 4. december 2024 været sendt i høring hos en række myndigheder, organisationer m.v. Materialet blev offentliggjort på Høringsportalen den 4. november 2024.

Digitaliseringsstyrelsen har på baggrund af høringen modtaget høringssvar fra i alt 7 organisationer og myndigheder.

Nedenstående parter har indsendt høringssvar med generelle og/eller tekstnære kommentarer:

- Regionernes IT-arkitekturråd
- Datatilsynet
- WAYF – Where Are You From
- Lakeside
- Erhvervsstyrelsen
- Statens IT
- Sundhedsdatastyrelsen

Alle tekstnære høringssvar fra de eksterne hørte parter er gengivet i deres fulde ordlyd i sektionen nedenfor. Digitaliseringsstyrelsens besvarelser og de specifikke ændringer, som er indført på baggrund af høringssvar, er nævnt i forbindelse med gennemgangen af høringssvarene.

OIOSAML 4 profilen er efter høringsfristen justeret på baggrund af høringssvarene fra ovenstående parter. Den endelige OIOSAML 4 profil publiceres på Digitaliseringsstyrelsens hjemmeside om OIOSAML i januar 2025.

Indholdsfortegnelse

Modtagne høringssvar og besvarelser fra Digitaliseringsstyrelsen 3

Regionernes IT-arkitekturråd 3
Datatilsynet 5
WAYF – Where Are You From 5
Lakeside 12
Erhvervsstyrelsen 20
Statens IT 22
Sundhedsdatastyrelsen 23

Ændringer på Digitaliseringsministeriets egen foranledning 25

Modtagne høringssvar og besvarelser fra Digitaliseringsstyrelsen

Regionernes IT-arkitekturråd

Bemærkning 1: Regionernes IT-arkitekturråd

RITA har identificeret nogle nøglepunkter, der kræver yderligere afklaring:
Login-processer:

- Sundhedsområdets systemer benytter specifikke sikkerhedsniveauer (LOAniveauer) til login. Der er behov for tilstrækkelig tid til at tilpasse disse til de nye krav i OIOSAML 4.
- MitID Erhverv: Der er usikkerhed om håndteringen af eIDAS-identiteter for erhvervsbrugere, fx dem med CVR-numre.

Behov for dialog og konkrete brugsscenarier:

De foreslåede ændringer kan påvirke fælles systemer, som regionerne og Sundhedsdatastyrelsen (SDS) bruger til brugeradministration, derfor vil RITA gerne understrege behovet for tæt samarbejde og koordinering med SDS og på tværs af regionerne med henblik på at sikre, at nuværende løsninger og tekniske profiler fortsat fungerer optimalt og understøtter fælles målsætninger. Derfor vil RITA opfordre Digitaliseringsstyrelsen til at afholde et dialogmøde med relevante høringsparter med henblik på, at få gennemgået ændringer sammen med konkrete brugsscenarier for ændringernes konsekvenser. Formålet med brugsscenarierne er, at hjælpe med at tydeliggøre, hvordan de foreslåede ændringer skal anvendes i praksis, og sikre, at ændringerne er relevante for de aktuelle behov.

Svar fra Digitaliseringsstyrelsen til bemærkning 1

Digitaliseringsstyrelsen er fuldt opmærksom på OIOSAML profilens brede anvendelse i den offentlige sektor, herunder sundhedssektoren. Derfor er der, som beskrevet i høringsbrevet, ingen aktuelle planer om at gøre profilen obligatorisk, og ibrugtagning af profilen er som udgangspunkt frivillig og behovsdrevet hos de enkelte sektorer og tjenesteudbydere. De grundlæggende ændringer består i understøttelsen af tjenesteudbydernes muligheder for at kunne modtage EU-identiteter, herunder at indføre et stærkere 'typebegreb' for identiteter, så det er lettere for en tjenesteudbyder at håndtere forskellige typer identiteter i samme løsning. Der kan naturligvis være EU-regulering, som pålægger den enkelte tjenesteudbyder at kunne modtage EU-identiteter, og her vil NemLog-in brokeren på sigt tilbyde en enkel måde at opfylde disse krav på gennem anvendelse af OIOSAML 4 profilen.

Det kan endvidere bemærkes, at OIOSAML 4 profilen i sig selv ikke ændrer på krav til sikringsniveauer (som defineres i NSIS og eIDAS). Sikringsniveauer er således helt uafhængige af autentifikationsprotokollen.

Vi har modtaget høringssvar fra andre aktører på sundhedsområdet (Sundhedsdatastyrelsen og Lakeside) og har tilrettet profilen i overensstemmelse med disse høringssvar. Hvis der er brug for yderligere afklaringer vedr. de tekniske ændringer i standarden, er Digitaliseringsstyrelsen åben for yderligere dialog.

Det skal dog understreges, at ansvaret for koordinering af overgang til den opdaterede profil ligger hos de enkelte sektorer og tjenesteudbydere.

Overgang til OIOSAML 4.0 profilen er helt frivillig og behovsdrevet, og NemLog-in brokeren vil i en lang periode understøtte både den nuværende OIOSAML 3.0.3 snitflade og den kommende OIOSAML 4 snitflade, hvorfor der ikke på kort sigt er nogen direkte påvirkning af Sundhedsområdets it-landskab.

Hvad angår MitID Erhverv er situationen pt. den, at en erhvervsbruger enten skal have et MitID (med eller uden CPR) eller være tilknyttet en Lokal IdP. Der er endnu ikke nogen fastlagte planer for, hvornår en erhvervsbruger eventuelt vil kunne anvende et eIDAS-anmeldt eID, og hvordan en sådan identitet vil blive repræsenteret attributmæssigt ved log-in gennem NemLog-in's broker.

Datatilsynet

Bemærkning 1: Datatilsynet

Datatilsynet bemærker, at tilsynet i forbindelse med høringen alene har forholdt sig til de it-tekniske forhold omkring OIOSAML 4 profilen, og tilsynet har således ikke forholdt sig til forhold, som måtte ligge ud over det rent tekniske. På baggrund af høringsdokumenterne har Datatilsynet forstået det således, at OIOSAML 4 profilen har været udarbejdet med udgangspunkt i det databeskyttelsesretlige princip om dataminimering. Datatilsynet har endvidere forstået høringsdokumenterne således, at de kryptografiske algoritmer og nøglelængder, der dels bruges på transportlaget (TLS-version 1.2 eller højere) og dels ved kryptering og signering af SAML Assertions, efterlever globalt anerkendte krypterings-standarder og algoritmer. På baggrund af ovenstående har Datatilsynet således ikke bemærkninger til den kommende version 4 af OIOSAML profilen.

Svar fra Digitaliseringsstyrelsen til bemærkning 1

Digitaliseringsstyrelsen kan bekræfte, at profilen er udarbejdet med udgangspunkt i princippet om dataminimering, og at kryptografiske operationer skal baseres på anerkendte algoritmer med tilstrækkelige nøglelængder. I forhold til algoritmer anvendt til transportsikkerhed (TLS) har styrelsen på baggrund af andre høringssvar valgt at inkludere referencer til CFCS' vejledning på området, som sikrer anvendelse af anerkendte krypteringsalgoritmer.

WAYF – Where Are You From

Bemærkning 1: WAYF

Vi har følgende bemærkninger til følgende punkter i høringsversionen af OIOSAML 4: **OIO-MD-03:** Hvorfor ikke samtidig kræve at certifikatet udstedes til netop den juridiske person der står bag entity'en, og ikke bare til en (hvilken som helst) juridisk person? Ellers får man måske ikke rigtig nogen sikkerhedsgevinst ved at bruge CA-certifikater.

Svar fra Digitaliseringsstyrelsen til bemærkning 1

Digitaliseringsstyrelsen anerkender baggrunden for ønsket, men det er samtidig styrelsens erfaring, at der i praksis ofte er brug for en vis fleksibilitet i certifikathåndteringen, fx når leverandører varetager it-systemer på vegne af tjenesteudbydere, eller når flere tjenesteudbydere har fælles it-systemer (herunder multi-tenant konstruktioner). Der er ofte i implementeringerne omkring metadatahåndtering supplerende sikkerhedsforanstaltninger, fx bliver administratorer autentificeret og autoriseret til at opdatere konfigurationen i NemLog-in's administrationsportal, og derfor vurderes en stramning af praksis ikke nødvendig. Digitaliseringsstyrelsen har derfor valgt ikke at ændre profilen på dette punkt – ellers skulle eksisterende implementeringer potentielt ud i en meget omfattende udskiftning af certifikater og metadata, hvilket vurderes uhensigtsmæssigt og uproportionalt med evt. gevinster.

Bemærkning 2: WAYF

OIO-SP-06: Styrelsens navn er nu: Agency for Digital Government.

Svar fra Digitaliseringsstyrelsen til bemærkning 2

Korrekt, der var tale om en manglende konsekvensrettelse i høringsversionen. Navnet er nu korrigeret.

Bemærkning 3: WAYF

OIO-SP-07: Hvis man vil bruge RequestedAuthnContext til at bede om attributprofiler og ikke kun om assurance levels, så fortolker man måske begrebet om RequestedAuthnContext bredere end hvad SAML-specifikationen kan bære. Vi læser nemlig SAML-specifikationen [SAMLCore] og https://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf sådan at RequestedAuthnContext specifikt er et ønske om et bestemt indhold af AuthenticationStatement'et og ikke har nogen relation til andre elementer i Assertion'en. Man kunne også få indtryk af at OIOSAML vil tillade SP'en at bede om en bestemt assurance level og en bestemt attributprofil i én og samme AuthnRequest, altså i én og samme RequestedAuthnContext. Er det tanken? I så fald er dét måske ikke decideret i modstrid med SAML-specifikationen — men det går måske heller ikke meget godt i tråd med specifikationens krav

om at IdP'en blandt de AuthnContextClassRef'er den understøtter, skal bruge den som står øverst i den prioriterede liste som RequestedAuthnContext er i en AuthnRequest (selv med erratum 45 rettet). Dvs. SAML-specifikationen [SAMLCore] lægger ikke op til at IdP'en i AuthnRequests skal forholde sig til mere end et enkelt element i listen. Og netop fordi listen er ordnet, er det overraskende at IdP'en ifølge første bullet i noten i OIO-SP-07 selv må bestemme hvilken af flere ønskede attributprofiler den vil svare med, og ikke SKAL svare med den første den understøtter.

Det er interessant at SAML-profilen for eIDAS på https://ec.europa.eu/digital-buildingblocks/sites/download/attachments/467109280/eIDAS%20SAML%20Message%20Format%2 0v.1.4.1_final.pdf har valgt at gå en anden vej og bruge RequestedAuthnContext kun til at bede om assurance levels og så defineret en Extension i AuthnRequest'en til at bede om attributter med — og på den måde undgået at overanstrenge RequestedAuthnContext-elementets semantik. Sidste bullet i noten i OIO-SP-07 er måske et symptom på at netop dét er sket hér — for hvorfor skulle der være værdier af RequestedAuthnContext som Comparison ikke giver mening for? Hvad er grunden til at man i OIOSAML ikke har overtaget eIDAS-SAMLs mere protokoltro måde at spørge om attributer på (altså vha. en Extension i AuthnRequest som emulerer metadatas RequestedAttribute-facilitet)?

Det er også interessant at man faktisk kan opnå hvad man vil her, helt uden at fortolke eller udvide standard-SAML, med brug af gammelkendte protokolelementer. I metadata kunne man nemlig lade hver SP definere et antal AttributeConsumingServices som hver har et Index og en så RequestedAttribute med navnet https://data.gov.dk/concept/core/eid/profile og attributprofil-URI'er som AttributeValues (jf. OIO-SP-35) — hvormed SP'en så i AuthnRequest'en ville kunne bede IdP'en om bestemte attributprofiler via AttributeConsumingServiceIndex. Den (konservative) løsning ville måske kræve færre tilpasninger i eksisterende SAML-software og kunne også overvejes.

Svar fra Digitaliseringsstyrelsen til bemærkning 3

Digitaliseringsstyrelsen har på baggrund af kommentaren besluttet, at oplysninger om den ønskede attributprofil flyttes fra RequestedAuthnContext elementet til en Extension i SAML requestet. Det er korrekt, at der kan være flere måder at kommunikere SP'ens ønsker til en IdP i autentifikationsanmodningen, herunder AttributeConsumingServiceIndex. I henhold til SAML skemaet kan en SP dog kun aflevere én sådan index-værdi per request, og det vil således ikke være muligt at udtrykke, at en autentifikationsanmodning gerne må besvares med flere forskellige typer identiteter (fx DK person og EU person). Det er derfor vurderingen, at brugen af den foreslåede Extension er den mest robuste mekanisme, der samtidig bedst matcher forretningsbehovet.

Bemærkning 4: WAYF

OIO-SP-08: Måske klarere med en mindre kompakt formulering som "using a private key corresponding to a public key in their metadata".

Svar fra Digitaliseringsstyrelsen til bemærkning 4

Den foreslåede præcisering er indarbejdet i profilen.

Bemærkning 5: WAYF

OIO-SP-09: Hvorfor ikke bare gøre base64-indkodning af ProviderName enten obligatorisk eller forbudt, så modtagerne af værdien kan vide sikkert hvordan den skal behandles (altså med eller uden base64-afkodning)?

Svar fra Digitaliseringsstyrelsen til bemærkning 5

Der har været ønsker i lidt forskellige retninger i høringssvarene i forhold til om ProviderName skal indkodes (se blandt andet bemærkning 5 fra Lakeside om samme emne). Digitaliseringsstyrelsen har på den baggrund valgt at gøre indkodning valgfri og dermed op til de konkrete implementeringer af profilen at aftale/beslutte.

Bemærkning 6: WAYF

OIO-SP-16: Formuleringen giver indtryk af at IdP'en altid skal besvare en AuthnRequest med en Assertion uanset om IdP'en kan honorere en evt. RequestedAuthnContext i AuthnRequest'en. Er dét tanken? I så fald kan man være bekymret for om SAML-specifikationen er overholdt. SAMLspecifikationen [SAMLCore] ser nemlig ud til at have et krav om at IdP'en besvarer en AuthnRequest med fejlen NoAuthnContext hvis ikke IdP'en kan honorere nogen af værdierne i AuthnRequest'ens RequestedAuthnContext-element.

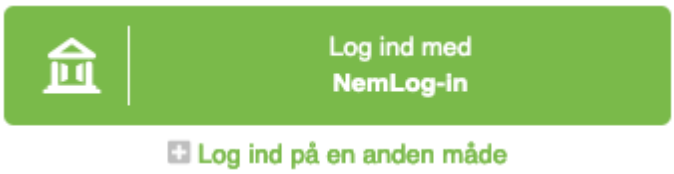
Svar fra Digitaliseringsstyrelsen til bemærkning 6

Det er ikke tanken, at en IdP altid skal besvare AuthnRequest med en Assertion, uanset om IdP'en kan honorere en eventuel RequestedAuthnContext i AuthnRequest'en. Der kan dog være implementeringer hos IdP'er, som fx i en single sign-on session vælger at udstede en Assertion, selvom ønsket LoA fra SP'en ikke kan honoreres. Hensigten med dette krav er at gøre det helt eksplicit, at det altid er SP'ens ansvar at tjekke LoA i Assertion, inden denne forlader sig på indholdet, således at SP'en ikke er afhængig af, hvordan IdP'en måtte være implementeret.

Bemærkning 7: WAYF

OIO-SP-17 og OIO-IDP-19: Mht. *discovery* vil vi henlede opmærksomheden på *Identity Provider Discovery Service Protocol and Profile* (se http://docs.oasis open.org/security/saml /Post2.0/sstc-saml-idp-discovery. pdf) samt RA21-knappen (se https://ra21.org), som tilsammen giver langt den bedste brugeroplevelse i forhold til dels at få direkte adgang til ens sædvanlige IdP, dels at have muligheden for at vælge om. Den onicielle implementering af RA21-knappen er "SeamlessAccess" (se https://seamlessaccess.org); men WAYF har lavet en implementering — "Mind the Gap" (se illustrationen nedenfor og https://wayf.dk/da/gui-f%C3%B8dereretlogin-standardiseret-internationalt) — som er tilpasset danske forhold. I denne sammenhæng betyder det at en bruger kan anvende forskellige IdP'er til forskellige tjenester. I WAYFs føderation for forskning og højere uddannelse er det normalt at man anvender sin institutions IdP til visse tjenester og NemLog-in til andre. Vi savner derfor også en beskrivelse af muligheden for at anvende elementet samlp:IDPList til at få en fælles discoverytjeneste til at fungere sammen med brokere — så SP'en kan fortælle brokeren hvilken bagvedliggende

"forretnings-IdP" brugeren har valgt i discovery'en, og brokeren sende brugeren derhen uden at brugeren skal foretage sig yderligere.



Svar fra Digitaliseringsstyrelsen til bemærkning 7

Digitaliseringsstyrelsen har besluttet at fjerne Discovery-afsnittet fra OIOSAML4, da håndteringen af dette vurderes at variere mellem føderationer og implementeringer. Det kan således bedre håndteres gennem lokal sub-profilering.

Bemærkning 8: WAYF

OIO-SP-34:
Det er overraskende at man vil have SP'er til at markere understøttelse af OIOSAML med en særlig værdi i protocolSupportEnumeration — i og med at OIOSAML tænkes som en profil af SAML2 og ikke som nogen særskilt protokol på niveau med SAML2, SAML1 osv.

Svar fra Digitaliseringsstyrelsen til bemærkning 8

Hensigten med eksplicit at angive understøttelse af V4 profilen i SP metadata er at gøre det lettere at understøtte migrering for IdP'er med mange tilsluttede tjenesteudbydere på tidligere versioner af profilen. Herved kan IdP'en entydigt ud fra metadata afgøre, om kommunikationen med en SP (og behandling af dennes metadata) skal ske efter den nye eller gamle profil.

Bemærkning 9: WAYF

OIO-SP-35:
Det er lidt uklart hvad formålet er når en SP angiver i metadata hvilke attributprofiler den "understøtter". Skal det opfattes som et signal til IdP'en om at den aldrig bør sende andre attributter til SP'en? Og/eller skal angivelsen forstås som et udsagn fra SP'en om at den altid vil kunne fungere uanset hvilken af de angivne profiler IdP'en vælger at sende?

Svar fra Digitaliseringsstyrelsen til bemærkning 9

Hensigten med angivelsen af de understøttede attributprofiler i SP metadata er at give IdP'en instruktioner om, hvilke typer identiteter som SP'en understøtter, det vil sige at IdP'en bør udstede en Assertion i henhold til en af disse typer. Digitaliseringsstyrelsen har i øvrigt valgt at flytte angivelsen til en metadata Extension for at imødekomme andre høringssvar.

Bemærkning 10: WAYF

OIO-IPD-21: Vi savner en beskrivelse af muligheden for at anvende Condition'en saml:OneTimeUse, som kendes fra de nyeste NemLog-in3-integrationsvejledninger. Understøttelse af SOAP-logout bør vel kun være obligatorisk hvis SP'en ikke altid bruger Condition'en saml:OneTimeUse, altså login uden sessionsdannelse? Generelt mener vi at SLO skaber større (sikkerheds)problemer end det løser. Dels pga. skrøbeligheden i frontend-protokollen, dels pga. brugernes manglende forståelse af hvad det er der foregår. Mens SingleSignOn er en convenience, er SingleLogOut en sikkerhedsrisiko — fordi den jo netop ikke logger en bruger ud af alle de sessioner vedkommende har, kun af dem som har brugt den pågældende IdP.

Svar fra Digitaliseringsstyrelsen til bemærkning 10

Digitaliseringsstyrelsen betragter OneTimeUse som en feature, der er specifik for NemLog-in, og ikke nødvendigvis er relevant i en fællesoffentlig profil med et bredere sigte. Andre IdP'er er naturligvis velkomne til at implementere funktionen, men det vil ikke være et hårdt krav i profilen. Det er i øvrigt korrekt, at single logout ikke er relevant for SP'er, som har anvendt OneTimeUse funktionaliteten, og dermed ikke deltager i en session. Dette er tilføjet som bemærkning til [OIO-SP-18]. Digitaliseringsstyrelsen er helt opmærksom på de udfordringer, som findes omkring robustheden af single logout mekanismen i SAML-føderationer. Funktionaliteten har historisk været til stede i alle versioner af OIOSAML og er stadig efterspurgt og relevant i en række scenarier, hvorfor styrelsen har valgt ikke at ændre noget på dette område.

Bemærkning 11: WAYF

OIO-AP-02:
Hvis her er tale om et begreb om samtykke som indebærer at samtykket skal kunne trækkes tilbage, hvordan kan brugeren så enektivt trække sit samtykke tilbage sådan at SP'en stopper med at bruge brugerens attributter?

Svar fra Digitaliseringsstyrelsen til bemærkning 11

Profilen foreskriver ikke specifikke mekanismer til indhentning eller tilbagetrækning af samtykker, men nævner blot mekanismen som en mulighed. Formuleringen er nu fjernet for at undgå forvirring omkring dette forhold.

Bemærkning 12: WAYF

6.6.2:
Hvorfor hér ikke bare holde sig til entityID'erne — som jo allerede er fastlagt i føderationen — frem for at åbne for at SP'er og IdP'er skal bruge kræfter på at aftale nye navne? Derudover har vi allerede AuthenticatingAuthority til at vise SP'en hvilke(n) IdP('er) brugeren loggede ind via. Forklaringen er måske at attributten er tænkt som den "inverse" udgave af AuthnRequest'ens ProviderName, dvs. den skal i tilfælde hvor der er brokere mellem SP og IdP, sørge for at "slut- SP'en" kan få et visningsnavn for "slut-IdP'en" uden at behøve metadata for slut-IdP'en at slå det op i?

Svar fra Digitaliseringsstyrelsen til bemærkning 12

Som det fremgår af teksten, er det helt op til den konkrete IdP at beslutte hvilke navne der giver mening i den lokale kontekst. Her kan der således anvendes EntityID'er som foreslået, hvis dette skønnes hensigtsmæssigt. Det er dog ikke sikkert, at et EntityID på en IDP giver mening for en SP, hvis der er en eller flere brokere imellem.

Lakeside

Bemærkning 1: Lakeside

3.2.2.1 Keys and Certificates
Under '[OIO-MD-03]' bør referencen til den nedlagte OCES2 løsning fjernes. Linket i fodnoten peger på et ligeledes nedlagt NemID site og bør opdateres.

Svar fra Digitaliseringsstyrelsen til bemærkning 1

Referencer er tilrettet til at pege på de seneste certifikatpolitikker.

Bemærkning 2: Lakeside

4.1.1.3 Authentication Contexts Eksemplet under [OIO-SP-06] benytter andre namespace præfikser end resten af dokumentet (hhv. 'saml2' i sted for 'saml' og 'saml2p' i sted for 'samlp') og bør ensrettes. Namespace deklarationen i eksemplet (xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion") bør fjernes for at øge læsbarheden og ensartetheden af eksemplerne.

Svar fra Digitaliseringsstyrelsen til bemærkning 2

Brugen af namespace prefixes er ensartet som foreslået, men dog beholdes name space deklarationen på AuthnConntextClassRef elementet for tydeligt at signalere, at dette element er deklareret i et andet namespace end det omgivende element.

Bemærkning 3: Lakeside

4.1.1.3 Authentication Contexts Til [OIO-SP-07]: Formålet med AuthnContextClassRef elementet er at lade SP'en angive et ønsket niveau (LoA) og/eller type af autentifikation, men ikke til at specificere hvilke attributter der ønskes af IdP'en (se SAML Core og SAML Authentication Context specifikationerne). I stedet bør der benyttes mekanismer til angivelse af ønskede attributter som anvender muligheder som er i overensstemmelse med SAML specifikationerne, fx 1. Anvendelsen af AttributeConsumingServices i SP-metadata kombineret med AttributeConsumingServiceIndex i AuthnRequest 2. Protocol Extension for Requesting Attributes per Request (se https://docs.oasis-open.org/security/saml-protoc-req-attr-req/v1.0/cs01/saml-protoc-req-attr-req-v1.0-cs01.html) I begge tilgange skal SP'en eksplicit angive hvilke attributter der ønskes, fremfor at angive et navngivet sæt af attributter som i den beskrevne tilgang. Det er ud fra et dataminimerings- og privacy-perspektiv mere hensigtsmæssigt, og burde måske endda være et krav, at SP'en kun rekvirer de attributter den har behov for, fremfor alle som hører til en bestemt attributprofil. Alternativt bør SAML extension meka nismen anvendes i AuthnRequest til at definere en måde hvorpå SP'er kan angive det ønskede attributprofil.

(NemLog-in IdP benytter allerede i dag SAML extension håndtaget til at understøtte AppSwitch på mobile platforme).

Det bemærkes, at allerede nuværende OIOSAML 3.0 benytter AuthnContextClassRef elementet til at lade en SP angive hvorvidt brugeren ønskes autentificeret som borger eller professionel, hvilket heller ikke helt er i tråd med SAML specifikationerne, hvor AuthContextClassRef bør som nævnt i ovenstående anvendes til skelne assurance levels og/eller autentifikationsmetoder.
(Borger/professionel muligheden var i øvrigt ikke med i OIOSAML 3.0 høringsversionen, men blev åbenbart efterfølgende tilføjet i den publicerede version.)

Svar fra Digitaliseringsstyrelsen til bemærkning 3

Digitaliseringsstyrelsen har ændret syntaksen, så informationen om ønsket attributprofil i stedet kommunikeres via et Extension element, således der ikke kan være tvivl om fortolkningen. Se dog svar til Sundhedsdatastyrelsens høringssvar om fortolkningen af, hvad elementet <RequestedAuthnContext> kan anvendes til i SAML standarden.

Styrelsen vurderer, at hensynet til dataminimering i OIOSAML 4 er tilgodeset på flere områder i profilen. For det første er det obligatoriske attributsæt (markeret med 'M' i tabellerne) meget smalt og indeholder ikke identificerende attributter – for DK person profilen er det fx kun specVersion og NSIS loa, der er obligatoriske. Øvrige attributter i DK person profilen (markeret som 'S' og 'O') er ikke obligatoriske og kan udveksles ved behov og efter aftale mellem IdP og SP, fx som angivet i metadata – i fuld overensstemmelse med ønsket om dataminimering. For det andet er værdierne af NameID attributterne aldrig globalt unikke, og for det tredje opererer profilen eksplicit med anonymiserede attributprofiler (frem for et eventuelt fravær af attributter), hvilket gør det enklere for tjenesteudbydere at håndtere scenarier med behov for høj privatlivsbeskyttelse.

I relation til forslaget med at anvende AttributeConsumingServiceIndex kan det bemærkes, at SAML skemaet ikke tillader fremsendelse af flere index værdier i et request, hvorfor mekanismen ikke kan anvendes til at forespørge om flere forskellige typer identiteter på én gang (fx DK person og eIDAS person). Dette vurderes at være et meget klart behov i den offentlige sektor ikke mindst i medfør af eIDAS forordningens krav om gensidig anerkendelse.

Det andet forslag med at benytte OASIS specifikationen (https://docs.oasis-open.org/security/saml-protoc-req-attr-req/v1.0/cs01/saml-protoc-req-attr-req-v1.0-cs01.html) har den ulempe, at en SP kun kan efterspørge foreningsmængden af attributter for de identitetstyper, de ønsker at modtage, ligesom det kan være komplekst at operere på foreningsmængder af attributter. Med mange slags identiteter i spil samtidig har styrelsen vurderet, at der skulle en ny konstruktion til i form af stærke typer.

Det har således været et klart designkriterie at definere nogle 'typer' af identiteter med veldefinerede attributsæt for at gøre det enklere for en tjenesteudbyder at håndtere, at man fx qua eIDAS-reguleringen kan være pålagt at modtage flere forskellige typer personer i samme løsning. Konstruktionen med attributprofiler giver en entydig måde at afgøre typen på (via profile attributten), således at det fx bliver let at skelne mellem en dansk person uden CPR og en EU person samt operere med særskilte forretningsregler til disse i en løsning.

Bemærkning 4: Lakeside

4.1.1.5 Proxy IdPs Til [OIO-SP-09]: Der antages, at navnet af den oprindelige SP også skal videreføres i scenarier med en kæde af proxy'er . Det kunne således med fordel præciseres, at en proxy ikke skal angive navnet af den foregående proxy men værdien af det modtagne ProviderName.

Svar fra Digitaliseringsstyrelsen til bemærkning 4

Forslaget er indarbejdet i profilen.

Bemærkning 5: Lakeside

4.1.1.5 Proxy IdPs Til [OIO-SP-09]: Hvad er formålet med at kræve base64-encoding af ProviderName? ProviderName skal jf. SAML Core være en 'human readable' streng og bør derfor ikke base64-encodes for at være compliant med SAML Core og sikre interopabilitet.

Svar fra Digitaliseringsstyrelsen til bemærkning 5

Formålet med encoding er at undgå tvivl om fortolkning af nationale specialtegn samt undgå udfordringer med tegn, der ikke er tilladt i XML. Kravet i SAML-standarden om at kommunikere en brugerrettet beskrivelse kan opfyldes, uanset om der benyttes encoding eller ej (brugeren ser jo ikke HTTP trafikken, men den tekst som IdP'er præsenterer i brugerfladen efter decoding). Det kræver naturligvis, at IdP og SP er enige om encoding. Styrelsen har ladet det være op til den konkrete implementering at beslutte, om der skal anvendes encoding.

Bemærkning 6: Lakeside

4.2 Single Logout Til [OIO-SP-18]: Det er uklart hvad der menes med sætningen 'The following requirements apply in the case of such support.' når en SP SKAL understøtte Single Logout Profilen. Kan sætningen slettes?

Svar fra Digitaliseringsstyrelsen til bemærkning 6

Ja, sætningen er slettet i profilen.

Bemærkning 7: Lakeside

5.4.2 Metadata Content [OIO-IDP-44] er ikke i tråd med SAML specifikationerne. I SAML Profiles specifikationen er en 'attribute profile' ikke et sæt af SAML attributter (som OIOSAML4 definerer det) men et regelsæt som definerer, hvordan attributter og deres værdier navngives og formateres. En IdP benytter således <AttributeProfile> elementet til angive overfor SP'er hvilke regler og formater den anvender til attributter (fx urn:oasis:names:tc:SAML:2.0:attrname-format:basic og/eller urn:oasis:names:tc:SAML:2.0:attrname-format:uri) Der bør derfor benyttes en anden mekanisme (out-of-band, SAML extension etc.) end <AttributeProfile> elementet til at kommunikere hvilke attributprofiler (efter OIOSAML definitionen) en IdP understøtter. Der bør også overvejes at benytte et andet begreb end 'attributprofiler' i OIOSAML.

Svar fra Digitaliseringsstyrelsen til bemærkning 7

Vi har ændret kravet til at benytte en metadata extension i stedet, så elementet <AttributeProfile> ikke 'strækkes' unødigt. Det sproglige begreb 'attributprofil' har været anvendt i OIOSAML siden version 2 (fx 'OCES Attribute Profile'), så selvom det potentielt kunne misforstås, vurderer styrelsen, at termen har 'vundet hævd' i dansk kontekst, og at en ændring ville kunne indebære udfordringer.

Bemærkning 8: Lakeside

Generelt om TLS
Under [OIO-SP-11], [OIO-IDP-03] og [OIO-IDP-29] kunne der med fordel peges på tilladte TLS algoritmer, så anvenderne ikke benytter algoritmer, som ikke længere vurderes som sikre. Og måske ville det også være passende at bede læserne om allerede nu at overveje Quantum-sikre TLS profiler?

Svar fra Digitaliseringsstyrelsen til bemærkning 8

Der er indsat en reference til CFCS' vejledning om sikker brug af TLS, som løbende opdateres i takt med den teknologiske udvikling.

Bemærkning 9: Lakeside

6 Attribut profiles og 6.2 Attribut profiles
Både afsnit 6 og underafsnittet 6.2 har samme overskrift, hvilket virker forstyrrende.

Svar fra Digitaliseringsstyrelsen til bemærkning 9

Overskriften til afsnit 6.2 er ændret.

Bemærkning 10: Lakeside

6.3 Shared DK attributes
SpecVer attribute (6.3.1) er også påkrævet i EIDAS profilerne jf. oversigtstabellen og er ikke begrænset til DK profilerne og bør derfor ikke stå i afsnit 6.3 Shared DK attributes.

Svar fra Digitaliseringsstyrelsen til bemærkning 10

Attributten er flyttet til afsnit 6.6 "OIO SAML 4 common attributes" for at imødekomme høringssvaret.

Bemærkning 11: Lakeside

6.4.1 PID attribute og 6.5.2 RID number attribute
Den kommende udfasning af PID og RID har givet en del anledning til forvirring hos mange anvendere. Der kunne med fordel angives hvilke andre ID'er SP'er bør anvende (fx en persistent UUID fra Subject NameID).

Svar fra Digitaliseringsstyrelsen til bemærkning 11

Digitaliseringsstyrelsen har indsat referencer til de attributter, som bør anvendes i stedet.

Bemærkning 12: Lakeside

6.6.6 CPR IAL Det er en general problemstilling at der i SAML ikke findes en standardiseret måde for at angive kilde og kvalitet af attributter (i modsætning til fx OpenID Connect, se https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html). CPR nummeret er særligt interessant i den beskrevne problemstilling omkring anvendelsen af en eID-Gateway, men det kan være lige så relevant i andre sammenhænge at kunne skelne mellem kilde/kvalitet/friskhed for andre attributter. Man kunne overveje at generalisere CPR IAL konceptet til et generisk 'attribut AL'. I SAML specifikationerne er det <Evidence> elementet som benyttes til at angive en yderlig kontekst omkring hvordan en identitet eller attribut er blevet verificeret. (<Evidence> mekanismen lader dog ikke til at være særligt anvendt i praksis).

Svar fra Digitaliseringsstyrelsen til bemærkning 12

Digitaliseringsstyrelsen er enige i, at der mangler en standardiseret mekanisme til angivelse af kvalitet for attributter i SAML standarden, og at <Evidence> mekanismen ikke lader til at have stor udbredelse. Behovet er tydeligt identificeret for CPR-attributten i regi af EU-identiteter, mens det ikke er fundet forretningsmæssigt begrundet at indføre mekanismen generelt – særligt i betragtning af den potentielle kompleksitet, det kunne medføre for anvenderne. Behovet er formentlig tydeligst for sektor-specifikke attributter, som netop ikke findes i specificeret i OIOSAML.

Bemærkning 13: Lakeside

6.6.7 Is robot En software robot bør have sin egen identitet, så det eksplicit fremgår at det ikke er en menneskelig bruger. Der er desuden risiko for at SP'er i overgang fra OIOSAML3 til OIOSAML4 overser, at de selv eksplicit skal tjekke for isRobot flaget. Forslag: Udvid '5.1.4 Subject Identifiers' men en tredje brugertype ('system'/'robot'/'device') ud over 'person' og 'professional', samt definer mekanismer til at angive at en robot agerer på vegne af en menneskelig bruger.

Svar fra Digitaliseringsstyrelsen til bemærkning 13

Digitaliseringsstyrelsen er enige i, at softwarerobotter bør have deres egen identitet samt egne identifikationsmidler og rettigheder, som er helt adskilt fra personidentiteter. Der er imidlertid et stærkt ønske om, at softwarerobotter skal kunne logge ind i legacy-applikationer (efter eksplicit og gensidig aftale mellem de pågældende tjenesteudbydere og brugerorganisationer), da det ofte er i legacy-applikationer, at behovet for automatisering via robotter er tydeligst. I moderne applikationer er det således langt bedre at anvende API'er til automatisering af arbejdsgange og processer, og her er robotter således overflødige. For at understøtte legacy applikationer vurderes det nødvendigt, at en robot kan få udstedt en Assertion med det forventede, bagudkompatible attributsæt, så applikationen ikke skal omskrives – men naturligvis udstedt på baggrund af autentifikation med en separat identitet. Det er netop ønsket om bagudkompatibilitet, som tænkes understøttet med isRobot attributten.

Bemærkning 14: Lakeside

6.7 eIDAS og 6.8 eIDAS Detalje: Profilen bør fastlægge regler, ikke beskrive en kommende håndtering i et deployment. Sætningen 'Note that the Latin script variant of values will always be provided so Service Providers do not need to handle transliteration.' bør derfor omformuleres.

Svar fra Digitaliseringsstyrelsen til bemærkning 14

Formuleringen hidrører fra diskussionen af 'transliteration' i eIDAS SAML specifikationerne, og Digitaliseringsstyrelsen har vurderet, at dette implementeringsvalg er relevant at kende for danske SP'er, så de kan indrette deres applikationer herefter. I modsat fald ville danske tjenesteudbydere blive udsat for en øget kompleksitet.

Bemærkning 15: Lakeside

7 References Detalje: En del af de angivne referencer bliver ikke anvendt i profilen og bør fjernes fra listen.

Svar fra Digitaliseringsstyrelsen til bemærkning 15

Der er ryddet op i referencelisten.

Erhvervsstyrelsen

Bemærkning 1: Erhvervsstyrelsen

Erhvervsstyrelsen har følgende to kommentarer ifm. OIOSAML4 høringen.

Vedrørende IDP-uafhængigt ID vil Erhvervsstyrelsen gerne høre Digitaliseringsstyrelsen ad ift. mulighederne for at NemLog-in kommer med et IDP-uafhængigt ID som er globalt på tværs af tjenesteudbydere og hvorfor det ikke er tænkt med som en del af den nye OIOSAML4 profil.

Nuværende situation: Persistent NameID er tjenesteudbyderspecifikt, og kan ikke bruges til at identificere brugere på tværs af løsninger/myndigheder

Forslag: Konkret vil Erhvervsstyrelsen foreslå, at "persistent" NameID ændres til faktisk at være globalt unikt, og ikke kun unikt for den aktuelle tjenesteudbyder. En særskilt attribut ville også være fint, så længe denne garanteres altid at være udfyldt.

Baggrund: Erhvervsstyrelsen oplever at mangle en fællesnævner mellem de forskellige tjenesteudbydere, således at det f.eks. i samarbejdet med andre myndigheder er tilstrækkeligt at sende det globale ID til at identificere brugeren på tværs af løsningerne. Et globalt ID, hvis udstillet, ville lette samarbejdet myndigheder imellem, da alle så kun har én parameter at forholde sig til, når brugere skal identificeres. Med andre ord: kompleksiteten i integrationer mellem myndigheder reduceres betydeligt.

Det ville derudover også lette kompleksiteten i myndighedernes individuelle løsninger betydeligt ikke at behøve forholde sig til flere ID'er. En kompleksitet som udelukkende stiger, ifm. at eID Gateway introducerer flere IDP-specifikke ID'er, som myndigheder skal forholde sig til.

Alternativet er det, man er nødsaget til i dag, nemlig at myndigheder naturligvis alligevel identificerer brugere unikt, blot via deres CPR-uuid (for personer), Persistent Identifier (for erhvervsbrugere) eller identifiers fra eIDAS, hvilket gør myndighedernes snitflader unødigt komplekse af samme årsag. Hertil hører en kommentar til sikkerhed, for da det allerede i dag er muligt unikt at identificere brugere via de IDP-specifikke ID'er, mener vi ikke at det globale ID bør have sikkerhedsmæssig impact

Vedrørende eID Gateway ændrer strukturen/formatet på adresser: I eID Gateway snitfladespecifikationen nævnes det, at eID Gateway ændrer strukturen/formatet på adresser: De udenlandske eIDAS middleware sender base64-encodede XML struktur, som således omformes af eID Gateway til et

simplificeret format (key/value par adskilt med ; og =). Er dette fortsat tilfældet?

Vi vil opfordre til, at denne formatændring ikke længere foretages, så tjenesteudbydere kan forholde sig til eIDAS Attributprofil i sin rene form, samt anvende relevante referenceimplementeringer og standarder fra europæisk hånd.

Svar fra Digitaliseringsstyrelsen til bemærkning 1

I forhold til den obligatoriske NameID attribut er det korrekt, at værdien af denne varierer per tjenesteudbyder. Baggrunden for dette er dataminimeringsprincippet og hensynet til brugernes privatliv, da et globalt unik ID ville kunne benyttes til at spore og sammenkæde en brugers færden på tværs af tjenester. Se i øvrigt også høringssvar fra Datatilsynet. Da NameID attributten er en obligatorisk attribut i SAML ville tjenester, som ikke har brug for 'globale' ID'er, blive pålagt at modtage dem.

De privatlivsvenlige egenskaber for NameID attributten har været gældende siden OIOSAML 3, og det vil potentielt have stor betydning for den offentlige sektor, hvis egenskaberne skulle ændres.

Digitaliseringsstyrelsen har derfor henlagt brugen af globale ID'er til de *frivillige* attributter i OIOSAML 4 profilen. Profilen understøtter således adskillige andre muligheder for globale, persistente identifiers på tværs af tjenesteudbydere, som kan tilvælges, når der er behov og hjemmelsgrundlag. Her kan fx peges på:

- https://data.gov.dk/model/core/eid/cprUuid
- https://data.gov.dk/model/core/eid/professional/uuid/persistent
- https://data.gov.dk/model/core/eid/cprNumber
- http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier
- http://eidas.europa.eu/attributes/legalperson/LegalPersonIdentifier
- https://data.gov.dk/model/core/eid/professional/rid (deprecated)
- https://data.gov.dk/model/core/eid/person/pid (deprecated)

Der er således rige muligheder for at operere med et persistent og globalt ID på tværs af tjenester.

I forhold til adresseattributter som

- http://eidas.europa.eu/attributes/legalperson/LegalPersonAddress
- http://eidas.europa.eu/attributes/naturalperson/CurrentAddress

henviser OIOSAML direkte til EU-specifikationerne [ESAML-AP] og anvender dermed de oprindelige værdier uden konvertering i eID gateway.

Statens IT

Bemærkning 1: Statens IT

Vi har ingen kommentarer udover at hvis implementeringen af OIOSAML 4 bliver obligatorisk på et senere tidspunkt, så vil vi gerne udbede os 3-6 måneders varsel, så vi kan have tid til at implementere eventuelle ændringer.

Svar fra Digitaliseringsstyrelsen til bemærkning 1

Digitaliseringsstyrelsen er opmærksom på, at en eventuel fremtidig ændring af status for profilen til obligatorisk vil kræve decentral implementeringstid og vil derfor i givet fald sikre en frist på minimum 6 måneder. Der er som nævnt i høringsbrevet ingen aktuelle planer om at gøre profilen obligatorisk.

Sundhedsdatastyrelsen

Bemærkning 1: Sundhedsdatastyrelsen

Indledningsvis vil Sundhedsdatastyrelsen (SDS) gerne takke for invitationen til at give svar på høring om OIOSAML4-profilen. Den internationale SAML-standard, den nationale OIOSAML-profil og sundhedsspecifikke sub-profileringer af OIOSAML benyttes bredt på sundhedsområdet. Uanset fremkomsten af nyere alternative standarder (Open-ID-Connect, OAuth2 etc.), vil SAML2-profiler i en årrække være en central del af adgangskontroller, såvel lokalt som nationalt og internationalt Sundhedsdatastyrelsen noterer derfor med tilfredshed, at OIOSAML-profilen fortsat vedligeholdes aktivt af Digitaliseringsstyrelsen.

Brugen af standarder har i de sidste 30 år været et centralt element i nationale strategier for at skabe interoperabilitet på sundhedsområdet. Med forordninger som EHDS (European Health Data Space) er fokus på interoperabilitet udvidet til at dække hele EU. Sundhedsdata-styrelsen noterer sig igen med tilfredshed, at OIOSAML bevæger sig i denne retning.

Summa summarum: Sundhedsområdets omfattende brug af markeds- og open-source-løsninger (og leverandørers behov for at kunne anvende gængse udviklingsværktøjer), samt behovet for at skabe fælles europæisk interoperabilitet, understreger behovet for at lade den nationale standardiseringsindsats ske indenfor rammerne af internationale standarder.

Som påpeget af virksomheden Lakeside (hvis høringssvar til OIOSAML4-profilen Sundheds-datastyrelsen er bekendt med), er der nogle områder, hvor OIOSAML4-profilen bryder med den bagvedliggende internationale SAML standard (mekanisme for attributprofiler, base64-encoding af ProviderName, Metadata Content etc.).

Såfremt Sundhedsdatastyrelsen som myndighed for anvendelse af it-standarder på sundhedsområdet, fortsat skal forpligte sundhedsvæsenets parter til at overholde OIOSAML-profilen, fordrer det at OIOSAML4 bringes i overensstemmelse med SAML. Alternativt må man forpligte parterne med overholdelse af profiler på sundhedsområdet, der overholder SAML, men som bryder med OIOSAML (hvilket vil være lidt ærgerligt).

Svar fra Digitaliseringsstyrelsen til bemærkning 1

Digitaliseringsstyrelsen påskønner det faglige samarbejde om de fællesoffentlige standarder og profiler, herunder anvendelsen på Sundhedsområdet, og vi vil naturligvis sikre, at den nye profil ikke har utilsigtede påvirkninger i sundhedssektoren.

Profilen er tilrettet ud fra de modtagne høringssvar, herunder flyttet angivelsen af de ønskede attributprofiler til 'Extensions' elementer, så der ikke er nogen tvivl om fortolkningen af disse elementer.

Digitaliseringsstyrelsen vil dog i den forbindelse gerne nævne, at man ikke finder, at de tidligere mekanismer i høringsversionen decideret 'brød' med SAML standarderne, som anført i høringssvaret - hverken syntaktisk eller semantisk. SAML Core specifikationen har fx følgende beskrivelse af det frivillige <RequestedAuthnContext> element:

> *If present, specifies a filter for possible responses. Such a query asks the question "What assertions containing authentication statements do you have for this subject that satisfy the authentication context requirements in this element?"*

Anvendelsen af elementet til at angive ønskede typer af identiteter lå efter Digitaliseringsstyrelsens opfattelse inden for den beskrevne anvendelse, nemlig at medsende 'autentifikationskontekst' der benyttes til at afgøre, hvilke typer assertions der ønskes udstedt. Som tidligere nævnt har vi desuagtet flyttet informationen til Extension elementer, så der ikke er nogen tvivl om fortolkningen.

Vi henviser i øvrigt til vores svar til LakeSide's høringssvar om samme emne.

Ændringer på Digitaliseringsministeriets egen foranledning

Digitaliseringsstyrelsen har parallelt med høringen selv arbejdet med profilen, herunder med implementering i den fællesoffentlige broker (NemLog-in) i forbindelse med integration af eID-gateway løsningen. Dette arbejde har valideret profilen samt givet feedback og indsigt, som ligeledes har givet anledning til følgende mindre opdateringer:

- De efterspurgte LoA-niveauer beskrevet i [OIO-SP-06] er ændret til generiske LoA-niveauer frem for NSIS-specifikke niveauer. Dette er sket for at understøtte, at en tjenesteudbyder kan efterspørge sikringsniveauer på en generel måde, der også dækker eIDAS-identiteter, i overensstemmelse med forordningens krav om gensidig anerkendelse. Det er ikke Digitaliseringsstyrelsens forventning, at danske myndigheder generelt har behov for at kunne forespørge et NSIS LoA separat fra samme eIDAS LoA, og i øvrigt kan understøttelsen for EU-identiteter konfigureres via metadata. Efterspørger en tjenesteudbyder fx et generisk LoA Betydelig for en DK Person identitet, vil svaret naturligt indeholde et NSIS-specifikt LoA.
- Den generiske LoA attribut er omdøbt til følgende identifier: https://data.gov.dk/concept/core/loa
- Kravet om understøttelse af AttributeQuery i [OIO-IDP-28] er ændret fra et 'SHOULD' til et 'MAY', da denne funktionalitet anvendes sjældent i praksis.
- Der er tilføjet en ekstra attributprofil for anonymiserede eIDAS personidentiteter (/Person/EU/Anonymous) helt analogt til den attributprofil, der findes for danske personidentiteter med navne- og adressebeskyttelse (/Person/DK/Anonymous). Den nye attributprofil kan anvendes til at understøtte scenarier, hvor en EU-personidentitet kan kobles til et dansk CPR-nummer, hvor der i CPR-registret fremgår med navne- og adressebeskyttelse.