DIGITALISERINGSSTYRELSEN

Høringsnotat

22. januar 2019

Behandling af indkomne høringssvar i forbindelse med den officielle høring af OIOSAML version 3.0

Digitaliseringsstyrelsen har ved høringsfristens udgang den 14. december 2018 modtaget en række høringssvar fra de organisationer og myndigheder, som fik tilsendt høringen. I alt er der modtaget høringssvar fra 13 organisationer og myndigheder, hvoraf 1 myndighed ikke havde kommentarer.

Høringsparternes besvarelser er i dette høringsnotat indarbejdet i ikke-redigeret form, så de følger strukturen i OIOSAML og ikke som samlede svar. Herved opnås et overblik over de samlede kommentarer til hvert punkt, hvilket giver læseren en bedre fornemmelse af, hvad andre evt. har svaret til de samme punkter.

De generelle kommentarer til OIOSAML er medtaget under punkt 1.

Der er generelt blevet taget vel imod opdateringen af OIOSAML.

God læselyst!

Indholdsfortegnelse

Generelle kommentarer

Afsnit	Generelt
Høringspart	ATP

Bemærkning	Fuldmagter benyttes af ATP's kunder til at tilgå selvbetjening på andres vegne, f.eks. regnskabsvirksomhed, som indberetter for sine kunder. Det er meget benyttet af virksomhederne i dag.
	
	ATP har også tidligere i år implementeret løsning for borgere; f.eks. kan en svagelig ældre give fuldmagt til en anden voksen, som kan varetage kontakten med det offentlige.
	
	Også fremover er der behov for at der bliver taget hånd om denne funktionalitet. Der skal i fremtidig løsning OIOSAML30 være en plan og model, som ATP ikke kan tolke af indeværende høringsmateriale.
	
	Definitionen ser således ud på Digitaliser 2.0.9 af OIOSAML
	
	`<bpp:PrivilegeList`
	`xmlns:bpp="http://itst.dk/oiosaml/basic_privilege_profile"`
	`xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >`
	`<PrivilegeGroup Scope="urn:dk:gov:saml:cvrNumberIdentifier:12345678">`
	`<Privilege>urn:dk:some_domain:myPrivilege1A</Privilege>`
	`<Privilege>urn:dk:some_domain:myPrivilege1B</Privilege>`
	`</PrivilegeGroup>`
	`<PrivilegeGroup Scope="urn:dk:gov:saml:seNumberIdentifier:27384223">`
	`<Privilege>urn:dk:some_domain:myPrivilege1C</Privilege>`
	`<Privilege>urn:dk:some_domain:myPrivilege1D</Privilege>`
	`</PrivilegeGroup>`
	`</bpp:PrivilegeList>`

	Det er nødvendigt for ATP at denne funktionalitet bibeholdes også i OIOSAML Web SSO Profile 3.0
Svar	Håndtering af privilegier herunder i form af rettigheder og fuldmagter ligger fortsat uden for OIOSAML-profilen og hører i stedet til i nabo-specifikationen 'OIO Basic Privilege Profile'. Digitaliseringsstyrelsen har ingen planer om at udfase eller ændre OIO Basic Privilege Profile på en måde, så ovennævnte forretningsbehov ikke fortsat vil blive tilgodeset.

Afsnit	Generelt
Høringspart	KOMBIT
Bemærkning	Generelt har mange elementer i standarden ændret navngivning som kræver en opdatering i samtlige systemer der anvender SAML. Det er en ekstra omkostning som der godt kunne være undgået hvis man i videst mulig udstrækning havde beholdt navngivning fra tidligere version af OIOSAML.
Svar	Digitaliseringsstyrelsen går ud fra, at der med kommentaren henvises til navngivning af attributter og svarer med dette som afsæt. Det er korrekt, at navnene på attributter er ændret i OIOSAML 3.0 ud fra flere hensyn bl.a. konsistens og ensartethed i navngivningen (OIOSAML 2.0.9 blandede flere tilgange til navngivning), på baggrund af skelen til struktur i navngivningen i eIDAS, og endelig ønsket om at følge de fælles retningslinjer for stabile http URI'er (se https://arkitektur.digst.dk/rammearkitektur/datastandarder/retningslinjer-stabile-http-urier). Med versionsskiftet i OIOSAML (2.0.9 => 3.0) signaleres, at der er tale om en ny major version, hvor ikke-kompatible ændringer indføres. Dette går samtidig hånd-i-hånd med de væsentlige ændringer, som følger af skiftet fra NemID til MitID, samt indførsel af en mere privacy-orienteret model, som bedre harmonerer med GDPR. Ved at indføre nye navne mindskes risiko for sammenblanding af de to profiler. Digitaliseringsstyrelsen vurderer, at attributnavne i en

	hensigtsmæssigt udført implementering bør være konstanter i koden, således at ændring af navnene i sig selv ikke bør være en større implementeringsopgave. Derimod vil udfasning af OCES-specifikke attributter som følge af overgangen fra NemID til MitID kunne forventes at give anledning til substantielle opdateringer af lokale implementeringer.

Afsnit	Generelt
Høringspart	Energinet
Bemærkning	Det må forventes, at SAML V2.0 Web Browser SSO Profile [SAML2Prof], udgives i endelig stabil version inden OIOSAML 3.0 frigives. Nuværende refererede SAML2Prof fra Kantara Initiative (https://kantarainitiative.github.io/SAMLprofiles/saml2int.html#SAML2Prof) er i version 0.05 Community Draft. Samtidig beskrives, om SAML 2.0 " This revision, the first major rewrite of this material", hvorfor det ikke kan udelukkes, at der stadig kan ske væsentlige ændringer af dokumentet.
Svar	Digitaliseringsstyrelsen er opmærksom på ændringer i SAML2Int profilen. Versionsnummeret på Kantara's hjemmeside indikerer, at der er tale om en tidlig alpha-version, hvilket er lidt misvisende, idet profilen er baseret på et langt forarbejde og indkorporerer erfaringer fra en række deployments og tidligere interoperabilitetsprofiler. Det vurderes derfor, at profilen udgør et solidt grundlag.

Afsnit	Generelt
Høringspart	Finans Danmark
Bemærkning	Finans Danmark støtter, at OIOSAML profilen opdateres for at understøtte de ændringer, der sker i næste generation af den fællesoffentlige infrastruktur til håndtering digitale identiteter. Det fremgår af høringsmaterialet, at NemLog-in3 forventes at benytte OIOSAML 3.0 som sin primære snitflade, når den går i drift i 2020. Det er Finans Danmarks forståelse at der i NemLog-in regi vil blive introduceret såkaldte 'lokale IdP'er' (Identity

	Provider). Det er i den forbindelse Finans Danmarks ønske til OIOSAML 3.0 profilen, at standarden muliggør, at en privat virksomhed under passende betingelser kan være lokal IdP. Vi ønsker, at virksomhedens medarbejdere dermed på basis af stærkt internt login og ved brug af en passende OIOSAML-ticket kan autentificere sig overfor (visse) offentlige systemer, samt at medarbejderens brugerrettigheder i det pågældende offentlige system kan være indlagt i den medsendte OIO- SAML-ticket.
Svar	Det er korrekt, at OIOSAML 3.0 vil være den primære snitflade, som udstilles af NemLog-in3-løsningen overfor tjenesteudbydere. Samtidig vil arkitekturen rumme mulighed for at lokale IdP'er kan tilsluttes til NemLog-in. Snitfladen mellem lokale IdP'er og NemLog-in er endnu ikke fastlagt i detaljer, men den forventes at blive baseret på en variant af OIOSAML 3.0.

Afsnit	Generelt
Høringspart	Danske Regioner
Bemærkning	Opfordring til at indhold ensrettes på tværs i relation til OIOSAML profil 3.0, fx ift. Referencearkitektur for brugerstyring.
Svar	Digitaliseringsstyrelsen vil overveje at opdatere referencearkitekturen for brugerstyring. Bemærk at denne dog har et bredere sigte end OIOSAML 3.0, hvorfor at krav i OIOSAML 3.0 godt kan være skærpede i forhold til en referencearkitektur, som skal dække flere scenarier.

Afsnit	Generelt
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Interne reference links (fx [XML-ENC]) peger på https://kantarainitiative.github.io/SAMLprofiles/saml2int.html i sted for referenceafsnittet.

Svar	Links til Kantaras side er fjernet.

Afsnit	Generelt
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Det er fint med at lade OIOSAML 3.0 tage afsæt i SAML2Int, men overvej en anden form for navngivning af normative krav for at holde OIOSAML adskilt fra SAML2Int (fx er [SDP-G01] ens i to profiler, mens [SDP-G02] har anden indhold)
Svar	Navngivningen er opdateret, så der ikke er overlap med kravnumre i SAML2Int profilen.

Afsnit	Generelt
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Det fremgår ikke i hvilke scenarier OIOSAML tænkes anvendt. Det kunne være formålstjenelig at tilføje et kort afsnit om brugsscenarier (fællesoffentlige, tværoffentlige, lokale, private aktørers anvendelser mfl.).
Svar	Der er tilføjet et afsnit til profilen, som uddyber anvendelsesscenarier. Bemærk dog, at forhold vedr. governance (hvilke organisationer skal leve op til hvilke standarder) bedre hører hjemme i referencearkitekturen for brugerstyring, som således kan pege på OIOSAML som en obligatorisk standard i visse situationer for visse organisationer.

1. Introduction

Afsnit	1.1
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Kontakt-email er angivet som nemlogin@digst.dk.

	Forslag: Brug en NemLog-in-neutral email-adresse for at signalere at profilen er uafhængigt af NemLog-in, fx oiosaml@digst.dk ☺
Svar	Forslaget er ikke implementeret.

2 Notation and terminology

Afsnit	2.2
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Der kunne med fordel tilføjes et par linjer om at en proxy-IdP optræder i SP rollen ift. andre IdP'er den føderer med.
Svar	Bemærkningen er indarbejdet i profilen.

3 Common requirements

Afsnit	3.1.1 Clock Skew
Høringspart	Danske Regioner
Bemærkning	Punktet er uklart formuleret. Punktet synes at tillade at implementeringen kan vælge vilkårligt fra +/- 3 minutter til +/- 5 minutter. Det er uklart, hvorfor skew-intervallet ikke er valgt til et enkelt bestemt område, f.eks. [-3 .. 3] minutter eller [-5 .. 5 minutter. Et simplere forslag ville være: Deployments MUST allow up to 5 minutes of clock skew ... etc. En alternativ forståelse er, at implementeringen skal forvente, at tids- punktet skal mindst være clock +/- 3 minutter og max være clock +/- 5 minutter. Denne forståelse giver dog ingen mening.
Svar	Kravet i profilen er præciseret til "Deployments MUST allow up

	to five (5) minutes of clock skew''.

Afsnit	3.1.1
Høringspart	Sundhedsdatastyrelsen
Bemærkning	'Clock Skew' på mellem 3 og 5 minutter virker noget stort i 2018. I praktiske SAML deployments anvendes sommetider token-*levetider* der kortere end det foreslåede 'clock skew'.
Svar	Erfaringer fra faktiske implementeringer (herunder NemLog-in føderationen) har vist, at det i praksis er nødvendigt at tillade et 'clock skew' i på flere minutter for at forhindre, at brugere afvises. Dette vurderes ikke at udgøre nogen sikkerhedsmæssig udfordring henset til de mange øvrige sikkerhedsmæssige tiltag i OIOSAML profilen.

Afsnit	3.1.3
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Forslag (detalje): Fjern 'saml' delen fra eksemplet. Det er måske lidt forvirrende ift. kravet fra nuværende NemLog-in (og OIOSAML 2.0?) om 'saml' præfikset i AssertionConsumerURL (som har voldt problemer i praktiske anvendelser)
Svar	Eksemplet er fjernet for at undgå misforståelser.

Afsnit	3.1.3 [SPD-G03]
Høringspart	Nets DanID
Bemærkning	Det var tidligere et krav, at entityID for Service Providere skulle anvende prefix 'saml'. Dette krav blev siden frafaldet. Høringsparten vil foreslå, at eksemplet i dette afsnit ikke anvender 'saml.' prefix, da det vil kunne forlede læser til at tro, at dette krav igen er gældende.

Svar	Eksemplet er fjernet for at undgå misforståelser.

Afsnit	3.2.2.1 Keys and Certificates
Høringspart	Danske Regioner
Bemærkning	Hvad lægges der i udtrykket "qualified certificates"? Testcertifikater? Andre udbydere?
Svar	Med 'qualified certificates' henvises til kvalificerede certifikater som defineret i eIDAS forordningen. Der er indsat en forklaring om dette i profilen.

4 SP Requirements

Afsnit	4.1.2.1, 5.1.1.1, 5.3
Høringspart	Datatilsynet
Bemærkning	Datatilsynet anmoder om, at det angives hvorvidt der er et minimumskrav til den anvendte version af TLS protokollen, og i så fald hvilken version der som minimum skal anvendes.
Svar	Der er tilføjet krav om brug af TLS version 1.2 eller højere.

Afsnit	4.2.1.2, 5.2.2
Høringspart	Datatilsynet
Bemærkning	Datatilsynet anmoder om, at en note tilføjes, der forklarer hvorfor `<saml:NameID>` elementet ikke må krypteres.
Svar	Der er tilføjet en note om dette. Hensynet er interoperabilitet, idet mange implementeringer ikke understøtter denne konstruktion.

Afsnit	4.1.1.3
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Dette er en meget hård binding til NSIS. Fællesoffentlige og tværoffentlige løsninger skal jf. Referancearkitektur for brugerstyring følge NSIS, men bør OIOSAML (og dens reference implementationer) ikke også kunne anvendes i andre (fx lokale) deployments? Forslag: Opblød kravet til at tillade andre klassifikationer til angivelse af ønsket LoA.
Svar	Det er Digitaliseringsstyrelsens hensigt, at profilen obligatorisk anvender NSIS sikringsniveauer (i Assertion), da dette er den fællesoffentlige danske standard. Bemærk dog, at det er frivilligt at angive det ønskede sikringsniveau i requestet. Kravet om at andre klassifikationer ikke må anvendes er reduceret til et "SHOULD NOT" fra et "MUST NOT".

Afsnit	4.1.1.5
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Kravet skaber hårde bindinger igennem infrastrukturen af proxy IdP'er - fremfor muligheden for at en mere løst koblet arkitektur lægges op til en model hvor tilslutninger af nye SP'er til fx en national proxy IdP påvirker lokale IdP'er. Samtidigt lægger kravet måske implicit op til at hvert login-request fra en SP skal sendes igennem hele kæden af proxy IdP'er, hvilket ikke nødvendigvis vil være den valgte tilgang i hvert deployment af profilen. Forslag: Drop kravet (eller reducer til MAY).
Svar	Digitaliseringsstyrelsen er ikke enig i, at formidling af navne (tekststrenge) giver arkitekturmæssige bindinger, da der ikke er snitflader eller integrationer mellem parter forbundet med en proxy. Det kan være nødvendigt at kende den 'reelle' SP af hensyn til at kunne håndhæve policies på IdP'en. Bemærk i øvrigt at kravet også har eksisteret i OIOSAML 2.0.9. Kravet er reduceret til et "SHOULD" fra et "MUST".

Afsnit	4.1.1.5 Proxy IdPs
Høringspart	KOMBIT
Bemærkning	[SDP-SP08] If the SP is in fact a proxy IdP acting on behalf of another SP, the service provider MUST include a element in the containing a element stating the Service Provider Identity uniquely. The RequesterID MUST uniquely identify the real service provider. **Svar** Det er KOMBITs erfaring at Microsoft AD FS ikke kan håndtere Scoping elementet når den modtages fra en proxy IdP, og desværre fejler AD FS med en teknisk fejl i brugergrænsefladen, og en besked i Windows loggen om at Scoping elementet ikke er understøttet. Det vil være uhensigtsmæssigt hvis OIOSAML 3.0 stiller et hårdt krav om at en proxy IdP skal anvende Scoping attributten - et SHOULD will være bedre her, så man kan håndtere anvendere af AD FS.
Svar	Bemærkningen er implementeret - kravet er reduceret til ”SHOULD” fra et ”MUST”.

Afsnit	4.1.1.3 Authentication Contexts
Høringspart	KOMBIT
Bemærkning	The following values MAY be used to request the desired [NSIS] assurance level, and if present, MUST be used with the Comparison attribute set to minimum: https://data.gov.dk/nsis/loa/Low https://data.gov.dk/nsis/loa/Substantial https://data.gov.dk/nsis/loa/High

	Note the implicit hierarchy between these levels. Other <samlp:AuthnContextClassRef> values MUST NOT be used. **Svar** Det er KOMBITs erfaring at Microsoft AD FS ikke kan håndtere <samlp:AuthnContextClassRef> elementet, når det modtages fra en Service Provider (eller Proxy IdP). I begge tilfælde fejler AD FS og viser en teknisk fejlbesked for slutbrugeren, og logger i Windows loggen at AuthnContextClassRef elementet indeholder en ikke-supporteret værdi. Microsoft har en liste af bestemte værdier som er lovlige, og disse indeholder ikke de nævnte LoA værdier. https://msdn.microsoft.com/en-us/library/hh599318.aspx
Svar	Digitaliseringsstyrelsen anerkender problemstillingen, og derfor er kravet formuleret som et 'MAY'-krav, således at man ikke er tvunget til at anvende funktionen. Udfordringen kan således løses ved at have registreret hvilken type IdP, man kommunikerer med, og undlade elementet, hvis den pågældende type IdP ikke understøtter det (eller ligefrem fejler, hvis det er indeholdt i requestet). Omvendt vurderes det at være særdeles relevant at kunne anmode om et bestemt sikringsniveau fra en IdP, som understøtter elementet. Herved kan undgås, at brugerne autentificerer sig (forgæves) på et for lavt sikringsniveau for herefter at blive afvist af tjenesten.

Afsnit	4.1.2.4 Forced Re-Authentication
Høringspart	Danske Regioner

Bemærkning	Kravet specificerer SHOULD – men kravets bemærkning taget til følge ville vel indebære et MUST?
Svar	Kravet er bibeholdt som et 'SHOULD' krav. Den omtalte bemærkning er misvisende og er derfor fjernet - se nedenstående.

Afsnit	4.1.2.4
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Til 'Note' delen: Kravet giver god mening, men vel af andre grunde (at sikre at IdP'en faktisk har honoreret ForceAuthn instruktionen): Requests fra SP'en er altid signeret jf. [SDP-SP07], så andre klienter kan ikke forfalske requests.
Svar	Bemærkningen er implementeret (noten er fjernet).

Afsnit	4.1.3
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Forslag: Opblød kravet til at tillade andre klassifikationer for LoA end NSIS. Se kommentar til 4.1.1.3
Svar	Det er Digitaliseringsstyrelsens hensigt, at profilen obligatorisk anvender NSIS sikringsniveauer (i Assertion), da dette er den fællesoffentlige danske standard. Bemærk dog, at det er frivilligt at angive det ønskede niveau i requestet, mens det er obligatorisk at angive i udstedt SAML Assertion.

Afsnit	4.1.3 LoA check
Høringspart	Styrelsen for It og Læring
Bemærkning	I forbindelse med tilvejebringelsen af næste generation af OIOSAML Web SSO Profile har Styrelsen for It og Læring med dette høringssvar et forretningsmæssigt fokus på mindreårige elevers digitale identitet i relation til udførelse af LoA tjek ud fra

	NSIS standarden. Den nuværende infrastruktur på Undervisningsministeriets område sikrer et stort og veletableret kendskab til alle institutionernes brugere. Dette har institutioner og offentlige og private tjenesteudbydere gavn af når de enten aftager eller udvikler digitale tjenester. Dette muliggør at unge under 15 år (pt. kun et-faktor login) kan få adgang til eksempelvis: digitale læremidler, nationale test, digitale afgangsprøver, elevplaner, skolens intranet etc. Samtidig giver det mulighed for at læreren, eller en anden ressourceperson på skolens område, inden for få minutter kan nulstille et glemt password. Implementering af OIOSAML 3 kommer potentielt til at have indflydelse på det kommende MitID og det kommende nye børneID. Disse vil supplere, og for børn over 13 år evt. erstatte, eksisterende løsninger på Undervisningsministeriets område. Styrelsen for It og Læring vil gerne indgå i en dialog om at definere håndteringen af mindreårige i forhold til NSIS's 'Low', 'Substantial' and 'High' niveauer. Dette for at sikre at skolebørn under 13 år ikke kun kan kvalificeres som 'begrænset' eller 'Lov' kategorien (ref. National Standard for Identiteters Sikringsniveauer). Samtidig skal det imødekommendes at et nyt BørneLogin, der er under udvikling, kan understøtte en to-faktorlogin, kan fungere med en step-up løsning hvor forældre eller lærer vil agere som anden faktor.
Svar	Digitaliseringsstyrelsen indgår gerne i en sådan dialog herunder om evt. alternative klassifikationer rettet mod børn under 13.

Afsnit	[SDP-SP30] – SP Requirements, Metadata and Trust Management
Høringspart	Erhvervsstyrelsen
Bemærkning	Bemærkning: Flere signeringscertifikater i brug samtidigt er en god idé, da det betyder mindre deploy-afhængigheder mellem IdP (NemLog-in) og Service Provider, når certifikater udskiftes.
Svar	Digitaliseringsstyrelsen er enig, og det nævnte forhold er netop baggrunden for udvidelsen af profilen.

Afsnit	4.3.2 [SPD-SP32]
Høringspart	Nets DanID
Bemærkning	Det er i dag et reelt problem at finde kontaktpersoner for de forskellige føderationsparter. Høringsparten vil derfor foreslå, at ønsket om SP's angivelse af kontakt- information skærpes til 'MUST'.
Svar	En skærpelse til 'MUST' ville betyde, at metadata uden kontaktinformation ville skulle afvises. I praksis vil nogle føderationer vedligeholde kontaktinformationer på anden måde end gennem metadata (fx i selvbetjeningsløsninger), og derfor kan dette blive en uhensigtsmæssig skærpelse.

5 IdP Requirements

Afsnit	5.1.4
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Det er meget hårde krav til NameID formater, som vil gøre det svært at benytte OIOSAML i andre fx lokale anvendelser og kravet vedrørende 'Format' forslås opblødet til SHOULD.
Svar	Bemærkningen er implementeret for så vidt angår kravet om UUID format.

Afsnit	5.2.1
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Der stilles kun krav til *modtagelse* af logout-requests (fra SP'er). Mangler der ikke et tilsvarende krav om bindings til *transmission* af

	LogoutRequest til SP'er?
Svar	Dette fremgår af krav [SDP-IDP21] (nu omdøbt til [OIO-IDP-21]).

Afsnit	5.2.1.1
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Skal modtagelse af SOAP logout request være *påkrævet*? SOAP baserede logout requests fra en SP gør det umuligt for IdP'en at initiere HTTP-Redirect eller HTTP-POST baserede logout requests til SP'er som ikke understøtter SOAP (da single logout er initeret uden for en user agent kontekst) og IdP'en kan dermed ikke gennemføre single-logout af aktive SP'er. SOAP-baseret SP-initieret logout giver kun mening hvis SP'er SKAL kunne modtage SOAP-bundne logout requests (men det er kun optionelt jf. [SDP-SP19])
Svar	Erfaringer fra NemLog-in-føderationen har vist, at det er urealistisk at forvente, at alle SP'er understøtter SOAP-baseret logout. Dette må derfor være et frivilligt for SP'er (som det i øvrigt er tilfældet med OIOSAML 2.0.9 i dag). Hensigten med profilens krav er, at IdP'en altid skal modtage det første logout-request via browseren for at kunne sende logout requests til de SP'er, som ikke understøtter SOAP-baseret logout. Når logout request skal sendes fra IdP til SP, kan IdP inspicere SP'ens metadata og vælge den mest robuste binding (eksempelvis prioritere SOAP binding over HTTP POST eller Redirect binding, som det er tilfældet i NemLog-in's aktuelle implementering). Kravene er blevet opdateret til at afspejle dette.

Afsnit	5.3.2 / [SDP-IDP36]
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Forslag: Tilføj for god ordens skyld at assertionen heller ikke må indeholde et <AuthzDecisionStatement>.
Svar	Elementet er tilføjet.

Afsnit	5.3.2
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Forslag: Tilføj et krav om at der kun må være et <AttributeStatement> på linje med kravet i [SDP-IDP11].
Svar	Dette er tilføjet.

Afsnit	5.4.2 / [SDP-IDP43]
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Detalje: Skriv 'should' med stort.
Svar	Dette er rettet.

Afsnit	5.4.2 [SPD-IDP42]
Høringspart	Nets DanID
Bemærkning	Sætningen "two <md:KeyDescriptor> element whose use attribute is set to signing and encryption" er en smule upræcis, og kunne med fordel rettes til "at least one <md:KeyDescriptor> element whose use attribute is set to signing and at least one <md:KeyDescriptor> element whose use attribute is set to encryption" - eller på anden vis præciseres.
Svar	Bemærkningen er indarbejdet.

6 Attribute Profiles

Afsnit	[SDP-AP04]

Høringspart	IBM (pva. Geodatastyrelsen)
Bemærkning	Brugen af ordet 'al' i sætningen '...be expressed as al <saml:AttributeValue> elements...' synes ikke at give mening.
Svar	Digitaliseringsstyrelsen kan ikke finde 'al' i sætningen. Der forekommer et 'al' i orddelingen af 'individual', men dette er hensigten.

Afsnit	6
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Overvej om der med fordel kunne opstilles en logisk model for attributter (semantik, værdirum, kardinalitet) som er uafhængig af SAML Web SSO (IdP'er, SP'er). Derved kunne samme logiske model også bindes til andre formater end SAML attributter, fx OAuth2 claims.
Svar	Digitaliseringsstyrelsen anerkender værdien i forslaget men vil vente med at implementere det, til behovet opstår (fx når flere beslægtede profiler får brug for at referere til samme attributter).

Afsnit	6
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Det er lidt uklart om profilen tillader andre (fx sektor-specifikke) attributter. Forslag: Tilføj eksplicit at andre attributter er tilladte.
Svar	Dette er tilføjet til kravet [OIO-AP-01].

Afsnit	6.1 / [SDP-AP01]
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Det er et noget snævert krav til IdP'er at skulle kunne udlevere alle nævnte attributter. Fx vil ProductionUnit, SENumber formentlig ikke være tilgængelig i alle IdP'er eller det vil ikke være behov for at

	kunne udstede bootstrap tokens i alle deployments. Forslag: Slet sætningen 'Conformant Identity Providers SHOULD be able to deliver all attributes regardless if they are marked as mandatory or not.'
Svar	Bemærkningen er implementeret.

Afsnit	6.1 / [SDP-AP04]
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Noget tekst ser ud til at være forsvundet, det bør formentlig stå *"…. a <saml:AttributeValue> be expressed as* ***sever**al <saml:AttributeValue> elements …"*
Svar	Bemærkningen er implementeret.

Afsnit	6.1 [SPD-AP04]
Høringspart	Nets DanID
Bemærkning	Sætningen "It is RECOMMENDED..." mangler noget i slutningen ifm. ordlyden "be expressed as al". Et eksempel kunne her være med til at tydeliggøre hensigten.
Svar	Bemærkningen er implementeret.

Afsnit	6.2.4
Høringspart	Nets DanID
Bemærkning	ID for Level of Assurance attributten angives som "https://data.gov.dk/nsis/LOA", mens der i afsnit 4.1.1.3 tales om værdierne "https://data.gov.dk/nsis/loa/Low" osv. Er det tilsigtet, at stavemåden er forskellige i de to afsnit ("LOA", "loa", hhv)?
Svar	Dette er hensigten, idet konventionen er, at sidste led i URI'erne skrives med stort, men prefix'et skrives med småt. Samme

	konvention benyttes i øvrigt i eIDAS SAML Attribute Profile. Forskellen i de nævnte eksempler består således i, at strengen 'loa' indgår på forskellige positioner.

Afsnit	6.2.4 (og 6.2.5 og 6.2.6)
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Det er igen hårde bindinger til NSIS, se kommentar til 4.1.1.3. Der kun med fordel åbnes for at kunne angive LoA som en angivelse af klassifikation (fx NSIS) op værdien i klassifikationen (encoded på passende vis).
Svar	Se tidligere svar; den obligatoriske anvendelse af NSIS er tilsigtet.

Afsnit	6.2
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Der er mulighed for at angive attributter for LOA, IAL og AAL. Er det et bevidst valg at federation assurance level (FAL) ikke er med? I deployments med proxy IdP'er kunne der måske give god mening at proxy IdP'en kunne angive forskellige FAL'er afhængigt af tilsluttede IdP'ers kapabiliteter.
Svar	I NSIS er FAL ikke en egenskab ved den autentificerede identitet (som LOA, IAL og AAL), men i stedet en statisk egenskab ved en IdP / Identitetsbroker. FAL anvendes ved autentifikation som et filter, således at en IdP ikke kan udstede Assertions med LoA, som et højere end dens eget FAL-niveau. FAL ville derfor høre bedre til i metadata end i Assertions.

Afsnit	6.2
Høringspart	Sundhedsdatastyrelsen

Bemærkning	Der kunne med fordel præciseres hvordan mellemnavne og flere fornavne bør håndteres.
Svar	En person skal i Danmark have mindst ét fornavn. Det er præciseret, at attributten kan indeholde flere fornavne afhængigt af implementeringen. Mellemnavne indgår ikke i attributten vedr. fornavn eller efternavn.

Afsnit	6.3
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Der savnes et attribut til angivelse af alder eller aldersgruppe, fx til SP'er med anonym rådgivning til unge, fora forbeholdt unge etc.
Svar	Attributten er tilføjet.

Afsnit	6.4
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Det er lidt uklart hvad der menes med 'related to the authentication context' i 6.4.3 til 6.4.6. Er det organisationen som har identitetssikret brugeren, autentificeret brugeren eller organisationen som brugeren repræsenterer?
Svar	Der menes den virksomhedskontekst (CVR), som brugeren agerer i. Dette er præciseret i profilen.

Afsnit	6.4.1
Høringspart	Datatilsynet
Bemærkning	Datatilsynet anmoder om, at der tilføjes en uddybende forklaring på, hvorfor en UUID for en professional role ikke er at betragte som en personoplysning.

Svar	Kravet går på, at UUID'en ikke må være den samme, når personen indgår i den professionelle rolle, i forhold til, når samme fysiske person optræder som privat. Dette for at skabe en datamæssig afkobling mellem de to situationer. Sagt på en anden måde, skal de to identiteter som den fysiske person ikke kunne korreleres gennem de UUID'er, som fremgår af IdP'ens Assertion. Profilen udtaler sig ikke om, hvorvidt UUID'en anvendt i den professionelle rolle er en personoplysning eller ej.

Afsnit	6.4.1
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Forslag: Fjern "which is persistent across all public sector SPs" idet UUID i sig selv er global unik (for alle praktiske anvendelser).
Svar	Hensigten er, at IdP'en med denne attribut udleverer samme UUID til alle SP'er for denne bruger, frem for at anvende SP-specifikke UUID'er. Formuleringen er præciseret, så dette fremstår tydeligere.

Afsnit	6.4.2
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Detalje: Eksemplet er i princippet en gyldig RID, men ligner mere en standard PID. Forslag: Ret til en 'standard-genereret' RID, fx 1231593107593
Svar	Bemærkning implementeret.

Afsnit	6.4.2
Høringspart	Nets DanID
Bemærkning	Det er uhensigtsmæssigt, at der i afsnittet angives et eksempel på et RID, som har PID syntax. Det kunne med fordel rettes til en

	mere gængs RID værdi, fx 8 cifre.
Svar	Bemærkning implementeret.

Afsnit	6.4.7
Høringspart	Sundhedsdatastyrelsen
Bemærkning	Samme semantik kunne udtrykkes i en OIOBPP struktur via Privileges_intermediate med et passende CVR scope og privilegie-navne. Forslag: Drop attributten og lad 'AuthorizedToRepresent' blive udtrykket i gennem OIOBPP strukturen på lige fod som fx borger-fuldmagter.
Svar	Forslaget anerkendes, men nuværende attribut er bibeholdt, da den også findes i eksisterende implementeringer.

Afsnit	6.2.4 Level of Assurance attribute
Høringspart	Danske Regioner
Bemærkning	Det fremgår af Referencearkitektur for Brugerstyring (side 73), at "Identitetsbrokere BØR kommunikere sikringsniveauet". Referencearkitektur for Brugerstyring bør tilpasses, således det fremgår at der er tale om SKAL (ikke bør) idet OIOSAML profil 3.0 foreskriver at LoA værdien er mandatory.
Svar	Digitaliseringsstyrelsen overvejer at tilpasse referencearkitekturen for brugerstyring ved passende lejlighed.

Afsnit	6.2.5 Identity Assurance Level attribute
Høringspart	Danske Regioner
Bemærkning	Værdien skal anvendes til beregning af LoA, det forekommer derfor nærliggende at lade den indgå i attributsættet som en

	mandatory del, idet det kan forventes at en/flere tjenesteudbydere på sigt vil skulle forholde sig til styrken af IAL.
Svar	Det er hensigten, at IdP'en skal beregne LoA i forbindelse med udstedelse af SAML Assertion, og derfor skal SP'en ikke selv beregne noget. Da IAL og AAL er nye begreber, vurderes som for tidligt at gøre disse attributter obligatoriske i profilen. Begge attributter vil kunne dog leveres af NemLog-in3's implementering.

Afsnit	6.2.6 Authentication Assurance Level attribute
Høringspart	Danske Regioner
Bemærkning	Værdien skal anvendes til beregning af LoA, det forekommer derfor nærliggende at lade den indgå i attributsættet som en mandatory del, idet det kan forventes at en/flere tjenesteudbydere på sigt vil skulle forholde sig til styrken af AAL.
Svar	Det er hensigten, at IdP'en skal beregne LoA i forbindelse med udstedelse af SAML Assertion, og derfor skal SP'en ikke selv beregne noget. Da IAL og AAL er nye begreber, vurderes som for tidligt at gøre disse attributter obligatoriske i profilen. Alle attributter dog vil kunne leveres af NemLog-in3's implementering.

Afsnit	6.3.1
Høringspart	UFST, Løsningsarkitektur og Test
Bemærkning	PID-attributten har status "deprecated" i den nye SAML profil, og det angives at tjenesteudbydere bør lægge planer for dens udfasning. Er der aktuelle planer for attributtens udfasning - eller måske en tidshorisont?
Svar	PID-attributten er snævert knyttet til den eksisterende OCES infrastruktur, som findes i relation til NemID. Med overgangen til

	MitID vil der ikke længere blive udstedt OCES personcertifikater, og derfor vil attributten udgå. Der kendes endnu ikke en præcis dato for udfasningen.

Afsnit	6.4.2 RID number attribute
Høringspart	UFST, Løsningsarkitektur og Test
Bemærkning	RID-attributten har status "deprecated" i den nye SAML profil og det angives at tjenesteudbydere bør lægge planer for dens udfasning. Er der aktuelle planer for attributtens udfasning - eller måske en tidshorisont?
Svar	RID-attributten er snævert knyttet til den eksisterende OCES infrastruktur, som findes i relation til NemID. I den nye identitetsinfrastruktur er det centrale begreb 'identiteter' og ikke certifikater (ikke alle erhvervsbrugere vil have et certifikat), og derfor udfases de attributter, som er tæt bundet op på certifikater. Der kendes endnu ikke en præcis dato for udfasningen.

Afsnit	6.4.2 RID number attribute
Høringspart	Danske Regioner
Bemærkning	Teksten skriver: "this attribute is deprecated and SPs SHOULD make plans...". I stedet for SHOULD så anbefales MUST.
Svar	Bemærkningen er implementeret.

Afsnit	[SDP-AP02] – Attribute profiles, General requirements
Høringspart	Erhvervsstyrelsen

Bemærkning	Spørgsmål: Hvis brugerne har mulighed for at udvælge, hvilke attributter de ønsker at sende til SP, betyder det så, at status på login er "Failed", hvis brugeren vælger at fravælge obligatoriske attributter?
Svar	Det vil afhænge af implementeringen men obligatoriske attributter vil normalt ikke kunne fravælges. Der er i øvrigt ganske få obligatoriske attributter i profilen.

Afsnit	6.2.4 Level of Assurance attribute
Høringspart	Erhvervsstyrelsen
Bemærkning	Spørgsmål: Hvis der indføres Identity Assurance Level (IAL) og Authentication Assurance Level (AAL) attributter, hvorfor så også introducere Level of Assurance (LoA), som disse to attributter reelt erstatter (se https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf)?
Svar	Ikke alle tjenesteudbydere kan forventes at kunne anvende både IAL og AAL til differentieret adgangsstyring, og derfor vil det for disse være bekvemt blot at kunne se på det samlede LoA. Bemærk i øvrigt at samlet LoA ikke nødvendigvis er minimum af IAL og AAL, idet fx NSIS krav til identitetsbrokere (NSIS kapitel 6) spiller ind på det samlede LoA, som Identitetsbrokeren må videreformidle.

Afsnit	6.3.1 PID attribute – Natural Person Profile
Høringspart	Erhvervsstyrelsen
Bemærkning	Spørgsmål: Hvis PID-attributten udgår, hvorledes identificeres en privatperson (natural person) så?
Svar	Privatpersoner kan identificeres gennem Subject (UUID) og evt. øvrige attributter som fx CPR og CPR UUID.

9. HØRTE PARTER

Nedenstående liste er en oversigt over de parter, der har indsendt høringssvar med generelle og/eller tekstnære kommentarer.

ATP

Danske Regioner

Datatilsynet

Energinet

Erhvervsstyrelsen

Finans Danmark

Geodatastyrelsen

KOMBIT

Nets DanID

Udviklings- og Forenklingsstyrelsen

Styrelsen for It og Læring

Sundhedsdatastyrelsen

Nedenstående har svaret, at der ingen kommentarer er til høringen:

Konkurrence- og Forbrugerstyrelsen