

Fælleskommunal OIOSAML 3 attributprofil

*OIOSAML 3-attributprofil for SAML 2.0 tokens i den
fælleskommunale infrastruktur*

1 Versionshistorik

Dokument version	Dato	Kommentarer
1.0	2024-03-18	OIOSAML-profiler er lagt ud som selvstændige dokumenter. Tidligere lå de i Appendiks D i Bilag 2_Vilkår for anvendelse af sikkerhedsmodellen i den fælleskommunale infrastruktur.pdf (digitaliseringskataloget.dk)

1.1 Indledning og vejledning

Denne udgave specificerer OIOSAML 3-profilen som implementeret af Context Handler 2.

I den fælleskommunale infrastruktur, baseres adgangsstyring på udstedelse og præsentation af såkaldte *security tokens*. Disse er XML-baserede billetter, der rummer information om en brugers eller et systems identitet, tildelte roller, autentifikation samt evt. anden information. Der henvises i øvrigt til Bilag 2A *Vilkår for anvendelse af sikkerhedsmodellen i den fælleskommunale infrastruktur* for en introduktion til den token-baserede model for adgangsstyring.

Med henblik på at sikre en ensartet håndtering af security tokens, der er interoperabel på tværs af teknologier og platforme, definerer dette appendiks en såkaldt attributprofil. Profilen specificerer obligatoriske krav til indholdet af security tokens, som anvendes i den fælleskommunale infrastruktur. Attributprofilen bygger videre på den fællesoffentlige OIOSAML-standard (se [OIOSAML] og [OIO-BPP]), og definerer således en kontrakt mellem udstedere af security tokens (Identity Provider og Security Token Services) og modtagere af security tokens (brugervendte systemer og fælleskommunale serviceudbydere). Denne profil består primært i en definition af hvilke SAML-attributter, der anvendes i den fælleskommunale infrastruktur, samt hvordan et Subject element formateres, og disse udvidelser vurderes at være interoperable. Der refereres eksplicit i kravene i disse underliggende profiler og standarder.

Bemærk, at krav til udformning af tokens har flere perspektiver:

- For Context Handler og Security Token Services angiver profilen, hvordan tokens skal opbygges.
- For modtagere af tokens (serviceudbydere og brugervendte systemer) beskriver profilen, hvilke typer tokens man skal kunne modtage og behandle.

1.2 Generelle krav

I dette afsnit beskrives generelle krav, som dækker alle typer tokens. For de enkelte token-typer angives i efterfølgende afsnit en række yderligere krav.

Tokens skal udveksles over transportmekanismer, der sikrer fortrolighed ved brug af stærk kryptering. Der henvises til Datatilsynets definition af stærk kryptering.

1.3 Brugertokens

I dette afsnit beskrives krav til brugertokens – dvs. tokens udstedt til en bruger, der er en medarbejder hos en Myndighed. Der findes to varianter af brugertokens:

- Brugertokens udstedt af en Myndigheds (lokale) Identity Provider, som indeholder brugerens jobfunktionsroller.
- Brugersystemtokens udstedt af Context Handler, som indeholder de systemroller, brugeren er tildelt for et specifikt it-system. Systemrollerne fremkommer ved at oversætte de jobfunktionsroller, som brugeren er tildelt hos en Myndighed, til de tilknyttede systemroller for det brugervendte system, der anmoder om tokenet. Oversættelsen mellem jobfunktionsroller og systemroller defineres af den enkelte Myndighed ved brug af Fælleskommunalt Administrationsmodul i den fælleskommunale infrastruktur.

Alle systemer i den fælleskommunale infrastruktur, som udsteder eller modtager brugertokens, skal overholde OIOSAML3-profilen [OIOSAML] af den internationale SAML 2.0-standard eller tilsvarende. Dette gælder således både regler ved udstedelse samt validering af tokens.

For indholdet af SAML-tokens gælder som udgangspunkt (medmindre andet nævnes eksplicit) kravene i OIOSAML3 kapitel 3 - 5 (fraregnet afsnit 5.3) men ikke kravene i de frivillige attributprofiler i OIOSAML kapitel 6 ("*Attribute Profiles*"). Her definerer dette dokument i stedet kravene til de SAML-attributter, der skal eller kan indlejres i tokenet.

Bemærk, at kravet ikke gælder eksterne Identity Providere som fx NemLog-in, hvor Context Handler vil foretage en veksling til KOMBIT's format defineret i denne profil.

1.4 SAML AuthnRequests

Context Handler 2 understøtter ikke angivelse af personprofiler jævnfør [OIO-SP-07] i OIOSAML 3, da der altid vil være tale om professionelle personer.

1.4.1 Subject Elementet

Subject elementet i SAML Assertions skal entydigt identificere medarbejderen i kontekst af en Myndighed.

Subject elementet skal indeholde et <NameID> element, der indkodes som et X.509 Distinguished Name med flg. elementer (dvs. OIOSAML3 afsnit 5.1.4 Subject Identifiers fraviges):

- Country (C) elementet skal indeholde ISO landekoden.
- Organization (O) elementet skal indeholde CVR-nummeret på den Myndighedskontekst, som tokenet er udstedt under.
- Common Name (CN) elementet skal indeholde medarbejderes navn. Dette behøver ikke være unikt i sig selv.
- Serial elementet skal indeholde et ID (tekststreng), der entydigt identificerer medarbejderen inden for Myndigheden.

Formatattributten på <NameID> elementet skal sættes til urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName.

Elementerne i Subject DN skal separeres med komma, og der må ikke være white space mellem elementer.

Nedenstående udgør et eksempel på et Subject Element i henhold til ovenstående krav:

```
<saml:Subject>
  <saml:NameID
    Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
    C=DK,O=19435075,CN=Hans Hansen,Serial=74c08b2b-212b-4f6d-9ce6-0fba1651087d
  </saml:NameID>
  <saml:SubjectConfirmation
    Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData
      Recipient="https://kombit.dk/Context Handler"
      NotOnOrAfter="2013-12-31T12:00:00"
      InResponseTo="Authn_request_identifier_1234567">
    </saml:SubjectConfirmationData>
  </saml:SubjectConfirmation>
</saml:Subject>
```

Bemærk, at Recipient URI'en i ovenstående eksempel er fiktiv og ikke nødvendigvis vil være den endelige værdi for Context Handler i den fælleskommunale infrastruktur.

Elementet <AttributeStatement> skal overholde indkodningsreglerne for attributter beskrevet i [OIOSAML3] afsnit 6. Desuden skal elementet indeholde nedenstående fælles attributter beskrevet i [OIOSAML3] afsnit 6.2 ('Common Attributes'):

- NSIS Loa – en klassifikation af, hvor stærk brugeren aktuelt er autentificeret af Identity Provideren i henhold til NSIS-standard (Low, Substantial, High), *eller*
- AssuranceLevel – en klassifikation af, hvor stærkt brugeren aktuelt er autentificeret (1-4) af Identity Provideren. Klassifikationen af AssuranceLevel skal følge sikringsniveauerne i NIST-standard. Denne anvendes midlertidigt for autentifikationer hidrørende for IdP'er, der endnu ikke understøtter NSIS-standard.
- SpecVer – angivelse af hvilken version af OIOSAML, der er anvendt ved udstedelse af tokenet.
- KombitSpecVer – angivelse af hvilken version af denne attributprofil, der er anvendt ved udstedelse af tokenet. For denne version af profilen sættes værdien til "2.0".

Bemærk, at de øvrige fællesattributter beskrevet i OIOSAML3 ikke er obligatoriske i denne attributprofil.

Nedenfor angives eksempler på de ovennævnte attributter:

```
<saml:Attribute
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
  Name="dk:gov:saml:attribute:AssuranceLevel">
  <saml:AttributeValue xsi:type="xs:string">3</saml:AttributeValue>
</saml:Attribute>
```

```
<saml:Attribute  
  
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
  
    Name="https://data.gov.dk/concept/core/nsis/loa">  
  
    <saml:AttributeValue xsi:type="xs:string">  
  
        Substantial  
  
    </saml:AttributeValue>  
  
</saml:Attribute>
```

```
<saml:Attribute  
  
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
  
    Name="https://data.gov.dk/model/core/specVersion">  
  
    <saml:AttributeValue xsi:type="xs:string">  
  
        OIO-SAML-3.0  
  
    </saml:AttributeValue>  
  
</saml:Attribute>
```

```
<saml:Attribute  
  
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"  
  
    Name="dk:gov:saml:attribute:KombitSpecVer">  
  
    <saml:AttributeValue xsi:type="xs:string">  
  
        2.0  
  
    </saml:AttributeValue>  
  
</saml:Attribute>
```

Bemærk, at den enkelte Identity Provider som følge af kravet er nødt til at klassificere det NSIS-sikringsniveau (LoA) eller NIST AssuranceLevel, som modsvarer styrken af den autentifikation, der

foretages af brugeren – samt indlejre værdien som en attribut i udstedte tokens. I vurderingen må man tage højde for både den tekniske styrke af autentifikationsmekanismen (fx kodeord, digital signatur etc.), relaterede tekniske kontroller (fx passwordpolitik, begrænsning af log-in til interne netværk etc.) men også for de organisatoriske procedurer, der er etableret til den indledende identifikation af brugeren (indrullering). Se [NSIS-standard] for detaljer.

Elementet <AudienceRestriction> i den udstedte SAML Assertion skal sættes til EntityID for det brugervendte system for tokens udstedt af Context Handler og til EntityID for Context Handler for tokens udstedt af lokale Identity Providere.

1.4.2 Attributter understøttet af Context Handler 2

Herunder findes en tabel med alle attributter for professionelle fra OIOSAML 3.0 med angivelse af, om den enkelte attribut er understøttet af Context Handler 2. I tabellen angiver "M" (Mandatory) obligatoriske attributter, som vil optræde i alle Assertions, og "O" (Optional) angiver attributter, som i visse tilfælde kan optræde i Assertions. Obligatoriske attributter skal medsendes lokale IdP'er til Context Handler.

Jævnfør OIOSAML3 skal alle attributter indkodes med:

NameFormat = "urn:oasis:names:tc:SAML:2.0:attrname-format:uri".

Attribute name	Context Handler 2 Support
https://data.gov.dk/model/core/specVersion	M
https://data.gov.dk/model/core/eid/privilegesIntermediate	O
https://data.gov.dk/concept/core/nsis/loa	O*
https://data.gov.dk/model/core/eid/email	O
https://data.gov.dk/model/core/eid/professional/uuid/persistent	O
https://data.gov.dk/model/core/eid/professional/cvr	M
https://data.gov.dk/model/core/eid/professional/orgName	M
https://data.gov.dk/model/core/eid/cprNumber	O

Og herunder er non-OIOSAML3 attributter understøttet af Context Handler 2:

Attribute name	Context Handler 2 Support
dk:gov:saml:attribute:AssuranceLevel	O*
dk:gov:saml:attribute:KombitSpecVer	M

Bemærk:

- Der skal enten angives et NSIS Loa eller NIST Assurancelevel.
- KombitSpecVer indkodes med NameFormat som "urn:oasis:names:tc:SAML:2.0:attrname-format:uri" (som øvrige attributter)
- AssuranceLevel indkodes med NameFormat som "urn:oasis:names:tc:SAML:2.0:attrname-format:**basic**"

1.5 Brugertokens med jobfunktionsroller

Brugertokens skal overholde de generelle krav beskrevet ovenfor og kan tillige indeholde de jobfunktionsroller, brugeren er tildelt. Hvis tokenet indeholder jobfunktionsroller, skal de repræsenteres i henhold til kravene i dette afsnit.

Jobfunktionsroller repræsenteres ved URI'er i et namespace lokalt for den organisation, der har defineret dem.

Nedenstående ses (fiktive) eksempler på URI'er for en jobfunktionsrolle i henhold til ovenstående krav:

- <http://odense.dk/roles/jobrole/sagsbehandler/1>
- <http://esbjerg.dk/roles/jobrole/leder/1>

Bemærk, at disse URI'er alene opfattes som identifiere, og at deres indhold i denne sammenhæng ikke er informationsbærende.

Jobfunktionsroller tildelt brugeren indkodes som privilegier i det udstedte SAML-token i henhold til OIOSAML Basic Privilege Profile [OIO-BPP]. I Scope attributten på privilegiet sættes CVR-nummeret for myndighedskonteksten.

Bemærk, at Scope-attributten enten kan indeholde brugerens egen myndighedskontekst eller konteksten for en fremmed myndighed. Hvis der angives konteksten for en fremmed myndighed, betyder det, at rollen er tildelt på vegne af denne myndighed via en delegering. Bemærk, at kontekst i Subject elementet ("O" elementet) altid indeholder kontekst for den myndighed, der har autentificeret brugeren.

Et eksempel på indkodning af en jobfunktionsrolle i henhold til ovenstående er:

```
<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:20374826">

    <Privilege>http://odense.dk/roles/jobrole/leder/1

    </Privilege>

  </PrivilegeGroup>

</bpp:PrivilegeList>
```

Dette element indlejres i en SAML-attribut ved at base64 indkode den og indsætte resultatet som en attributværdi (se [OIO-BPP] for detaljer):

```
<saml:Attribute FriendlyName="Privileges"

  Name="dk:gov:saml:attribute:Privileges_intermediate"

  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">

  <saml:AttributeValue xsi:type="xs:string">

    <!-- Her indsættes den base64 indkodede værdi -->

  </saml:AttributeValue>

</saml:Attribute>
```

1.6 Brugersystemtokens med systemroller

Brugersystemtokens skal overholde de generelle krav beskrevet ovenfor og kan tillige indeholde de brugersystemroller, brugeren er tildelt til det brugervendte system, der har anmodet om tokenet. Hvis tokenet indeholder brugersystemroller, skal de repræsenteres i henhold til kravene i dette afsnit.

Brugersystemroller repræsenteres ved URI'er i et namespace specifikt for det it-system, de er tilknyttet.

Nedenfor ses (fiktive) eksempler på URI'er for brugersystemroller i henhold til ovenstående krav:

- http://sapa.kombit.dk/roles/usersystemrole/se_sag/1
- <http://sapa.kombit.dk/roles/usersystemrole/adgang/1>

Bemærk, at disse URI'er alene opfattes som identifiere, og at deres indhold i denne sammenhæng ikke er informationsbærende.

Dataafgrænsninger skal repræsenteres på flg. måde:

- Dataafgrænsningen indlejres i et <Constraint> element. Der kan angives flere sideordnede <Constraint> elementer, og den resulterende dataafgrænsning skal opfattes som fællesmængden af disse udført på alle systemroller i samme <PrivilegeGroup> element.
- Navnet på dataafgrænsningen angives som en "Name" attribut på elementet indeholdende en URI i et namespace specifikt for det it-system eller den organisation, den er tilknyttet.

Værdien på dataafgrænsningen udtrykkes som en tekststreng.

Nedenstående eksempler viser et fiktivt eksempel på dataafgrænsninger påtrykt en systemrolle:

```
<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:20374826">
    <Constraint Name="http://sts.kombit.dk/constraint/kle/1">25.*</Constraint>
    <Constraint Name=" http://sts.kombit.dk/constraint/foelsomhed/1">Medium</Constraint>
    <Privilege>http://sapa.kombit.dk/roles/usersystemrole/se_sag/1</Privilege>
  </PrivilegeGroup>
</bpp:PrivilegeList>
```

Semantikken af ovenstående skal forstås sådan, at brugeren er tildelt systemrollen ("se_sag"), der er underlagt dataafgrænsningerne "KLE=25.*" og "følsomhed=medium". Bemærk, at Scope attributten (som tidligere) indeholder den anvenderkontekst, som rollen er tildelt under. Hvis rollen er delegeret fra en anden myndighed, vil CVR-nummer i Scope indeholde den delegerende myndigheds CVR-nummer.

Brugersystemroller tildelt brugeren indkodes som privilegier i det udstedte SAML-token i henhold til OIOSAML Basic Privilege Profile [OIO-BPP] dvs. de indlejres i attributten "dk:gov:saml:attribute:Privileges_intermediate". I Scope attributten på privilegiet sættes CVR-nummeret for myndighedskonteksten.

1.7 Servicesystemtokens

Servicesystemtokens (herefter kaldet servicetokens) minder meget om brugersystemtokens, men indeholder identitet og systemroller tildelt et Anvendersystem fremfor en personbruger. Servicetokens udstedes altid til brug for kald af en specifik, fælleskommunal service og vil derfor

kun indeholde de systemroller, der er defineret af denne service. En anden forskel er, at servicetokens af sikkerhedsmæssige grunde kun kan præsenteres ved samtidig signering med anvendersystemets private signaturnøgle (et såkaldt "holder-of-key" token). Endelig kan det nævnes, at servicetokens rekvireres fra Security Token Service ved brug af WS-Trust-protokollen frem for SAML-protokollen, som anvendes ved brugertokens.

Alle systemer i den fælleskommunale infrastruktur, som udsteder eller modtager servicetokens, skal overholde "OIO Profile for Identity Tokens" [OIO-IDT] af den internationale SAML 2.0-standard.

Der bør ikke anvendes kryptering på <Assertion> elementet eller dets del-elementer.

Bemærk: Servicetokens i denne profil bærer alene Anvendersystemets identitet og rettigheder, og der medtages ikke information om en evt. bagvedliggende bruger, selvom dette er muligt med OIO-profilen. Termen "invocation entity" i OIO-profilen skal derfor forstås som Anvendersystemet ved anvendelse af denne profil.

Vedrørende kryptering: Profilen er designet til brug med underliggende transportmekanismer, der sikrer fortrolighed ved brug af stærk kryptering. Anvendelse af meddelelsesbaseret kryptering er derfor fravalgt, da det ikke vurderes at give en øget sikkerhed, men derimod ville give forøget kompleksitet og svartider. For brugertokens anvendes kryptering af SAML Assertions (i henhold til krav i OIOSAML) fordi disse tokens kommunikerer via brugerens browser og potentielt kan indeholde personoplysninger.

Subject elementet i SAML Assertions skal entydigt identificere Anvendersystemet inkl. den organisation, det er udstedt til.

Subject elementet skal derfor indeholde et <NameID> element, der indkodes som et X.509 Distinguished Name. Værdien af dette sættes til Subject feltet fra Anvendersystemets System eller Organisations-certifikat¹, der på forhånd er registreret i Fælleskommunalt Administrationsmodul og anvendt til at signere anmodningen om tokenet med (WS-Trust).

Elementet <AttributeStatement> skal overholde indkodningsreglerne for attributter beskrevet i [OIOSAML] afsnit 7.2. Desuden skal elementet indeholde nedenstående kerneattributter:

- AssuranceLevel – en klassifikation af, hvor stærkt anvendersystemet aktuelt er autentificeret (1-4) af Identity Provideren. Klassifikationen af AssuranceLevel skal følge [NSIS]. System eller Organisations-certifikater er pt. klassificeret til niveau 3.
- KombiSpecVer – angivelse af hvilken version af denne attributprofil, der er anvendt ved udstedelse af tokenet. For denne version af profilen sættes værdien til "2.0".

Bemærk: De øvrige kerneattributter beskrevet i OIOSAML anvendes ikke i denne attributprofil.

Elementet <AudienceRestriction> i den udstedte SAML Assertion sættes til EntityID for den service (Web Service Provider), som tokenet er requestet til.

¹ OCES2-certifikater fra NemID Erhverv eller OCES3-systemcertifikater udstedt af MitID Erhverv.

Servicesystemroller repræsenteres ved URI'er i et namespace specifikt for den service, de er tilknyttet.

Nedenfor ses (fiktive) eksempler på URI'er for servicesystemroller i henhold til ovenstående krav:

- <http://organisation.kombit.dk/roles/servicesystemrole/rediger/1>
- <http://organisation.kombit.dk/roles/servicesystemrole/udstil/1>

Bemærk, at disse URI'er alene opfattes som identifiere, og at deres indhold i denne sammenhæng ikke er informationsbærende.

Dataafgrænsninger skal repræsenteres på flg. måde:

- Dataafgrænsningen indlejres i et <Constraint> element. Der kan angives flere sideordnede <Constraint> elementer, og den resulterende dataafgrænsning skal opfattes som fællesmængden af disse udført på alle systemroller i samme <PrivilegeGroup> element.
- Navnet på dataafgrænsningen angives som en "Name" attribut på elementet indeholdende en URI i et namespace specifikt for det it-system eller den organisation, den er tilknyttet.

Værdien på dataafgrænsningen udtrykkes som en tekststreng.

Nedenstående eksempler viser et fiktivt eksempel på dataafgrænsninger påtrykt en systemrolle:

```
<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:20374826">
    <Constraint Name="http://sts.kombit.dk/constraint/kle/1">25.*</Constraint>
    <Constraint Name="http://sts.kombit.dk/constraint/foelsomhed/1">Medium</Constraint>
    <Privilege>http://organisation.kombit.dk/roles/servicesystemrole/rediger/1</Privilege>
  </PrivilegeGroup>
</bpp:PrivilegeList>
```

Bemærk: Introduktionen af <Constraint>-elementet er nyt i forhold til Basic Privilege Profile. Semantikken af ovenstående skal forstås sådan, at Anvendersystemet er tildelt systemrollen ("rediger"), der er underlagt dataafgrænsningerne "KLE=25.*" og "følsomhed=medium". Bemærk, at Scope attributten (som tidligere) indeholder den anvenderkontekst, som rollen er tildelt under. Hvis rollen er delegeret fra en anden myndighed, vil CVR-nummer i Scope indeholde den delegerende myndigheds CVR-nummer.

Servicesystemroller tildelt Anvendersystemet indkodes som privilegier i det udstedte SAML-token i henhold til OIOSAML Basic Privilege Profile [OIO-BPP] dvs. de indlejres i attributten

"dk:gov:saml:attribute:Privileges_intermediate". I Scope attributten på privilegiet sættes CVR-nummeret for myndighedskonteksten (den myndighed, som rettigheden er tildelt på vegne af). Ved delegeringer af rettigheder fra en fremmed myndighed, vil indholdet være den fremmede myndigheds CVR-nummer.

1.8 Eksempel på brugersystemtoken

Nedenfor ses et ikke-normativt eksempel på et brugersystemtoken udstedt af Context Handler. I fald der er afvigelser i forhold til de formelle krav, er det kravene, der tager præcedens.

```

1  <Assertion ID="idb93be5b329964fdbbeef0317bed781eb"
2      IssueInstant="2023-09-13T07:10:02.590Z"
3      Version="2.0"
4      xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
5  >
6      <Issuer>https://saml.kombitoces3.safewhere.local/runtime/</Issuer>
7      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
8          <SignedInfo>
9              <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
10             <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
11             <Reference URI="#idb93be5b329964fdbbeef0317bed781eb">
12                 <Transforms>
13                     <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
14                     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
15                 </Transforms>
16                 <DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256" />
17                 <DigestValue>uonRVwsN00S7q/DRcdmqJW/uf8Ag4C+fbWPxgVblfPk=</DigestValue>
18             </Reference>
19         </SignedInfo>
20         <SignatureValue>mu7TKAcnnV0nQyEY80d+NINxh08j3cqirsquzqpW9wGrvsNJkX0DRbqS6XqbtRU/
21         CBcRlrQfaHC0Nq93a8D2njI0t1Zfy8LWqXm0dg+jsBdEdhe4ZaU6WP02bgF9iKMR+vD1stH70/
22         1s6JrT5agbESSRY+Q1QQbU8wk54xNvzz+RffQBAunagwQDVInLjWihNvdhHfB582KjtbKNAVnFPrqIMuYR/pD40v+DDfy19Ka0i/
23         B5zMYr+WXqoWeGSsxS00Kl6oQ/H+vLIQc7Mh550e0DsRSRlWxqkTPmRa2T+PkeJAJ19w44qxRs66bYxmbYv3KWR2Gspg7ZEMSEh0ffgyZlwvrcYFk7K
24         rNQdQHL0ysE47Izp3i0KxvWouGni23qi3dRRY0FGLusUTnwGwbbhpmQlWf5AznL8HafC8me08cfkM/
25         L2ffvUhn+votaiPpRY9tBr2HUGAg+Kw7eMgmC+8rbYWHh82EmR81CQ6A5Uk7fL0zco0/XUZ</SignatureValue>
26     </Signature>
27     <KeyInfo>
28         <X509Data>
29             <X509Certificate>MIIGozCCBNegAwIBAgIUBpsF5YA6gu3uX1i3TSYEJIfNqAgwQYJYKoZIHvCNAQEKMDSGDzANBgghkgBZQMEAgEFAKEC
30             MBoGCSqGSIb3DQEBDQANBgghkgBZQMEAgEFAKIDAgEgMGSxLTArBgNVBAMtJERlbjEYEW5za2UgU3RhdCBPQ0VTHVhkc3RlZGVuZGUtQ0EgM
31             TETMBEGA1UECwwKVGVzZCATIGN0aTEYMBYGA1UECgwPRGVuIERhbnNzSBTdGF0MQswCQYDVQGEWJESzAeFw0yMjE0MzVaFw0yNT
32             ExMjEwOTF0MzRaMIGeMRUwEwYDVQQDDAxtQUMiFnpZ25pbmcxNzA1BgNVBAUTLlVJOkRLLU86RzplN2EyOTZhZi1lYWQ5LTRlNmUtOGIyMCI
33             jYtQzZTFkZWl4OTAxJjAkBgNVBAoMHVRlL3RvcmdhbmlyYXRyY24ubnIuIDk3MDcxMzU4MRcwFQYDVQRhDA50VFJESy05NzA3MTM1ODEMAKGA
34             A1UEBhMCRESwggGiMA0GCsGSIb3DQEBQUAAIBjYAwggKAAoIBgQDN+Af8KkwPJRA4JEXunykcMxZuNw0QoY835Wffvz7s2gaIqPsl1aNNL
35             BoovTKX0i1Qq+LTXrPZGcFxtNLXJCuhRn4AhTcrrFeK00Twi8RmswUuKq2Ufv9eS24jYnDrr8C1/
36             oXbTp65PnrQwml1d1EUzPZqL1DaZWAmCdwSBm3qbncVmNyeDGsJ/
37             FvAKuU9LKhVzEzjFmzAnp44pD3A9u0ee8MF+RezsVti2v0uZhKcXkdZHyngghGPI/fgLToq8pBpSLcsTbubj3yzb+SMuViSgYgTvd6w5nMuA
38             VbXh1nXQ+EEQlbq70jUCJGxVR8hAQfXs0L6JWwLgDghoeWl7y9tsxI6H2QKKBQUXDrs41AuMKT6PfXcGLoijqsgdS6LFHENwu7A9G2mDjmdh
39             3Fz4GGFx9RTv8NmPZC5M8AgKU60SDqSro+kqkXZuoRuE02N9BBag1XAE6WybLHE6VjExexh5pV009jIDvRDWJXN0hfgq60YA09ASZxM
40             kf0dMCwAAEaA0CAAEwggGdMAwGA1UdEwEB/wQCMAAwHwYDVDR0jBBgwFoAUfyif2XGZQuj159c1di5NCCVtdl4wewYIKwYBBQUHAQEebzBtME
41             MGCCsGAQUFBzAChjdodHRwOi8vY2E5LnM0aS1nb3YuZGsvb2Nlcyp3c3N1aW5nLzEvY2FjZXJ0L2lzc3VpbmcuY2V5MCIYDQYDZDQEBABhBg
42             odHRwOi8vY2E5LnM0aS1nb3YuZGsvb2Nlcyp3c3N1aW5nLzEvY2FjZXJ0L2lzc3VpbmcuY2V5MCIYDQYDZDQEBABhBg
43             KQEBAAQMHMDsGCCsGAQUFBwEDBDB8wLTArBggrBgEFB0cLajAFAfBgEC4IvS0ECMBSGEmh0dHBzO18vdWlkLmdvd15kzBF8gNVHR8EPjA8MDQgQ
44             KA2hjRodHRwOi8vY2E5LnM0aS1nb3YuZGsvb2Nlcyp3c3N1aW5nLzEvY2FjZXJ0L2lzc3VpbmcuY2V5MCIYDQYDZDQEBABhBg
45             CgxRjSlJA0BgNVHQ8BAf8EBAMCBeAwQYJYKoZIHvCNAQEKMDSGDzANBgghkgBZQMEAgEFAKECMB0GCSqGSIb3DQEBDQANBgghkgBZQMEAgE
46             FAKIDAgEgA4IBgQDG/06RTgX4MOCC+ISzd+YXoT9sh8yDwbH4Waw6soi/
47             zLCPA0Zjy1RUEDTRLHYhejmRheL900syMke98UiuwLiLa7TKRGNrIV7oVUZZ8bsiY/
48             vECnLZY9wWAD5GVPMrF1H8KnRYRoEvv6MFgFgGKa+UfbFavjMSUmTxHp09RMWK+ThWyc85vkNUoppge4cu/
49             N2Jf26ncjncEjxe7ZJMVrl7kGKWgCaAniwbStE28Shg2UgnfHoP2wA91I22R8ibCmIA2hApJe93QtW3PajVlPnFQnd7cfk/
50             RhRyTfSd1n8lk2bdvYQofEt0/ef7HkpFPsTL63eDhzb12FxeXKWhztL9+EcwF29yWwL2QGUtj8TI5FY0KdGk63jwEKyRslUf905G5D6NxtR
51             i6i6IGi11vLkeghLVma1ngILT8cu6k6guxpLIMB1v0E6HF5pCnXDCYlpG/
52             ftI2avShpM23jwN8ZFkLN5eenPhVlkfNby4mKYkoEC0REL5cf/MpA=</X509Certificate>
53         </X509Data>
54     </KeyInfo>
55     <Signature>
56     <Subject>
57         <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">C = DK, O = 19435075, CN = user1
58         oces3kombitdp, Serial = 555ed208-2ed1-4739-8d79-119908219311</NameID>
59         <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
60             <SubjectConfirmationData InResponseTo="ide3663fa813054cee9dc9abdb4d33a986"
61                 NotOnOrAfter="2023-09-13T07:15:02.590Z"
62                 Recipient="https://oces3saml2wif3kombitnsis.safewhere.local/login.ashx"
63             />
64         </SubjectConfirmation>
65     </Subject>

```

```

36 <Conditions NotBefore="2023-09-13T07:10:02.590Z"
37     NotOnOrAfter="2023-09-13T07:15:02.590Z"
38     >
39         <AudienceRestriction>
40             <Audience>https://oces3saml2wif3kombitnsis.safewhere.local/</Audience>
41         </AudienceRestriction>
42     </Conditions>
43     <AuthnStatement AuthnInstant="2023-09-13T07:10:02.590Z"
44         SessionIndex="WUKV1sgEnIInouAlAhVpwQ=="
45         >
46             <AuthnContext>
47                 <AuthnContextClassRef>https://data.gov.dk/concept/core/nsis/LOA/Substantial</AuthnContextClassRef>
48                 <AuthenticatingAuthority>https://saml.oces3kombitdp.safewhere.local/runtime/</AuthenticatingAuthority>
49             </AuthnContext>
50         </AuthnStatement>
51         <AttributeStatement>
52             <Attribute Name="https://data.gov.dk/concept/core/nsis/LOA"
53                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
54                 >
55                 <AttributeValue>Substantial</AttributeValue>
56             </Attribute>
57             <Attribute Name="https://data.gov.dk/model/core/eid/email"
58                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
59                 >
60                 <AttributeValue>user1@gmail.com</AttributeValue>
61             </Attribute>
62             <Attribute Name="https://data.gov.dk/model/core/specVersion"
63                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
64                 >
65                 <AttributeValue>OIO-SAML-3.0</AttributeValue>
66             </Attribute>
67             <Attribute Name="dk:gov:saml:attribute:KombitSpecVer"
68                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
69                 >
70                 <AttributeValue>2.0</AttributeValue>
71             </Attribute>
72             <Attribute Name="https://data.gov.dk/model/core/eid/professional/cvr"
73                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
74                 >
75                 <AttributeValue>19435075</AttributeValue>
76             </Attribute>
77             <Attribute Name="https://data.gov.dk/model/core/eid/professional/orgName"
78                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
79                 >
80                 <AttributeValue>KOMBIT A/S</AttributeValue>
81             </Attribute>
82             <Attribute Name="https://data.gov.dk/model/core/eid/privilegesIntermediate"
83                 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
84                 >
85                 <AttributeValue>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluc2Z0eXVVRGLGtPz48YnBwOlByaXZpbGVnZUxpc3QgeG1sbmM6YnBwPSJodHRwOi8vZGlnclnc3QvZGsvb2lvc2FtbC9iYXNpY19wcml2aWxlZ2VfcHJvZmZlZSIsIGeG1sbmM6eHNpPSJodHRwOi8vd3d3LnczLm9yZy8yMDAxL1hNTFNjaG VtYS1pbmN0Wj5ZI+PFBYaXZpbGVnZUdyb3VwIFNjb3B1PSJ1cm46ZG6Z2920cnNhbw6Y3ZyTnVtYmVSWRlbnRpZmllcjoxOTQzNTA3NiI+PFBYaXZpbGVnZU5odHRwOi8va29tYm0LmRrL3JvbGVzL3VzZXJzeXN0ZWlyb2x1LT2vtbvWpdHJvbGxlcXNC8xPC90cm12aWxlZ2Uu+PENvbnn0cmFpbnoG TmfTzT0iaHR0cDovL2tvbWJpdC5kay9jb25zdHJhaW50cy9LEUUVNCI+S0xFLzQwMDAwMTwwQ29uc3RyYWludD48L1ByaXZpbGVnZUdyb3VwPjxQc m12awxlZ2VhcmlrcBTY29wZT0idXJ0OmRr0mdvdjpzYW1s0mN2ck51bWJ1cklkZWS0aWZpX2XiMTk0MzUwNzYiPjxqcm12aWxlZ2Uu+aHR0cDovL2 tvbWJpdC5kay9yb2x1cy91c2Vyc3lzdGVtcms9S29rb21iaXRyb2xsZTUvMTwwUHJpdmJsZwdLPjxB25zdHJhaW50IE5hbWU9Imh0dHA6Ly9rb21 iavQvZGsvY29uc3RyYWludHMvS0xFLzQ1PktMR580MDAwMDE8L0NvbnN0cmFpbnoQ+PC90cm12aWxlZ2VHCm91cD48UHJpdmJsZwdLR3JvdXAguU2Nv cGU9INvybjpkazpnbs3Y6c2FtdDpjdnJ0dW1iZXJZGVudG1maWVy0yE5NDM1MDC3Ij48UHJpdmJsZwdLPmh0dHA6Ly9rb21iaXQuZGsvcm9scXMvd XNlcnN5c3RlbnR3JvbGVuVa29tYm0cm9sbGU2LzE8L1ByaXZpbGVnZT48Q29uc3RyYWludCB0YW11PSJodHRwOi8va29tYm0LmRrL2NvbnN0cmFpb nRzl0tMR581Ij5LEUUVNTAwMDAwPC90b25zdHJhaW50PjxB25zdHJhaW50IE5hbWU9Imh0dHA6Ly9rb21iaXQuZGsvY29uc3RyYWludHMvS0xFLzUw IPktMR581MDAwMD8L0NvbnN0cmFpbnoQ+PENvbnn0cmFpbnoQTmfTzT0iaHR0cDovL2tvbWJpdC5kay9jb25zdHJhaW50cy9LEUUVNSI+S0xFLzUw MDAwMzwvQ29uc3RyYWludD48L1ByaXZpbGVnZUdyb3VwPjxqcm12aWxlZ2VhcmlrcBTY29wZT0idXJ0OmRr0mdvdjpzYW1s0mN2ck51bWJ1cklkZ WS0aWZpX2XiMTk0MzUwNzciPjxqcm12aWxlZ2Uu+aHR0cDovL2tvbWJpdC5kay9yb2x1cy91c2Vyc3lzdGVtcms9S29rb21iaXRyb2xsZTUvMTwwUH JpdmJsZwdLPjxB25zdHJhaW50IE5hbWU9Imh0dHA6Ly9rb21iaXQuZGsvY29uc3RyYWludHMvS0xFLzU1PktMR581MDAwMDE8L0NvbnN0cmFpbno Q+PENvbnn0cmFpbnoQTmfTzT0iaHR0cDovL2tvbWJpdC5kay9jb25zdHJhaW50cy9LEUUVNSI+S0xFLzUwMDAwMjwwQ29uc3RyYWludD48Q29uc3Ry YWludCB0YW11PSJodHRwOi8va29tYm0LmRrL2NvbnN0cmFpbnoRzl0tMR581Ij5LEUUVNTAwMDAwPC90b25zdHJhaW50PjxwUHJpdmJsZwdLR3Jv dXA+PFBYaXZpbGVnZUdyb3VwIFNjb3B1PSJ1cm46ZG6Z2920cnNhbw6Y3ZyTnVtYmVSWRlbnRpZmllcjoxOTQzNTA3NiI+PFBYaXZpbGVnZU5odH RwaW50cy9LEUUVNSI+S0xFLzUwMDAwMzwvQ29uc3RyYWludD48L1ByaXZpbGVnZUdyb3VwPjxwYnBwOlByaXZpbGVnZUxpc3Qv+</AttributeValue>
86     </AttributeStatement>
87     </Assertion>

```

1.9 Referencer

[NSIS-standarden]	"National Standard for Identiteters Sikringsniveauer (NSIS)" Version 2.0.2a National Standard for Identiteters Sikringsniveauer (NSIS) (digst.dk)
[OIOSAML]	"OIO Web SSO Profile V3.0.3" https://digst.dk/it-loesninger/standarder/oiosaml-profiler/
[OIO-BPP]	"OIO Basic Privile Profile V1.2" https://digst.dk/it-loesninger/standarder/oiosaml-profiler/
[OIO_IDT]	"OIO Identity Token Profile V1.2" https://digst.dk/it-loesninger/standarder/oio-identity-based-web-services-12-oio-idws/