KOMBIT

# *Fælleskommunal OIOSAML 2 attributprofil*

*OIOSAML 2-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.<br><br>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

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.

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).

Bemærk, at denne profil bygger på OIOSAML 2.1.0, hvor sikringsniveauer ikke følger NSIS-standarden men i stedet [NIST-standarden]. NSIS-standarden er således først taget i anvendelse med OIOSAML 3.0.

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 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.

Alle systemer i den fælleskommunale infrastruktur, som udsteder eller modtager brugertokens, skal overholde OIOSAML-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 kravene i OIOSAML afsnit 7.1 og 7.2 (”*Authentication Assertion Profile*”) men ikke kravene i de frivillige attributprofiler i OIOSAML kapitel 8 (”*OCES attribute profile*”) samt kapitel 9 (”*Persistent Pseudonym Attribute Profile*”). Her definerer dette dokument i stedet kravene til de SAML-attributter, der skal 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.

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:

- 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 indenfor 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 [OIOSAML] afsnit 7.2. Desuden skal elementet indeholde nedenstående kerneattributter beskrevet i [OIOSAML] afsnit 7.3:

- AssuranceLevel – en klassifikation af, hvor stærkt brugeren aktuelt er autentificeret (1-4) af Identity Provideren. Klassifikationen af AssuranceLevel skal følge sikringsniveauerne i [NIST-standarden].
- 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 "1.0".

Bemærk, at de øvrige kerneattributter beskrevet i OIOSAML ikke er obligatoriske i denne attributprofil.

Nedenfor angives eksempler på de to 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">2</saml:AttributeValue>

</saml:Attribute>
```

```
<saml:Attribute

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

        Name="dk:gov:saml:attribute:SpecVer">

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

          DK-SAML-2.0

       </saml:AttributeValue>

</saml:Attribute>
```

```
<saml:Attribute

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

        Name="dk:gov:saml:attribute:KombitSpecVer">

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

          1.0

       </saml:AttributeValue>

</saml:Attribute>
```

Bemærk, at den enkelte Identity Provider som følge af kravet er nødt til at klassificere det 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 [NIST-standarden] for detaljer.

Elementet <AudienceRestriction> i den udstedte SAML Assertion 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.

### 1.3.1 Attributter understøttet af Context Handler 1 og 2

Herunder findes en tabel med attributter fra OIOSAML 2 med angivelse af, om den enkelte attribut er understøttet af Context Handler. 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. Blank angiver, at attributten aldrig forekommer. Obligatoriske attributter skal medsendes fra lokale IdP'er til Context Handler.

**Context Handler 1:**

| Attribute name | Context Handler 1 Support |
|---|---|
| urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName[1] | M |
| dk:gov:saml:attribute:AssuranceLevel | M |
| dk:gov:saml:attribute:SpecVer | M |
| dk:gov:saml:attribute:KombitSpecVer | M |
| dk:gov:saml:attribute:Privileges_intermediate | M |
| dk:gov:saml:attribute:CvrNumberIdentifier | M |

**Context Handler 2:**

| Attribute name | Context Handler 2 Support |
|---|---|
| urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName | M |
| dk:gov:saml:attribute:AssuranceLevel | M |
| dk:gov:saml:attribute:SpecVer | M |
| dk:gov:saml:attribute:KombitSpecVer | M |
| dk:gov:saml:attribute:Privileges_intermediate | M |
| dk:gov:saml:attribute:CprNumberIdentifier | O* |
| https://data.gov.dk/model/core/eid/professional/uuid/persistent | O** |
| dk:gov:saml:attribute:CvrNumberIdentifier | M |

Bemærk, at AssuranceLevel attributterne har værdier i intervallet [1-4] i henhold til [NIST-standarden] og [OIOSAML] 2, idet NSIS-sikringsniveauer først er taget i brug med OIOSAML 3.

*CPR anvendes til at lave step-up mod NemLog-In 3 med MitID Erhverv.

**MitID Erhvervs UUID er en krævet attribut, hvis en bruger skal logge på et system via Sundhedsvæsenets Elektroniske Brugerstyring (SEB).

[1] Er strengt taget ikke en attribut i <AttributeStatement> element, men en del af Subject elementet.

## 1.4 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 identifiers, 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>
```

## 1.5 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 identifiers, 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>
```

Bemærk: Introduktionen af <Constraint>-elementet er nyt i forhold til Basic Privilege Profile. 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.

## *1.6 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 kommunikeres 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-certifikat, 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 [NIST-standarden]. System eller Organisations-certifikater er pt. klassificeret til niveau 3.
- KombitSpecVer – angivelse af hvilken version af denne attributprofil, der er anvendt ved udstedelse af tokenet. For denne version af profilen sættes værdien til ”1.0”.

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.

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 identifiers, 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.

## *1.7 Eksempel på brugersystemtoken*

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

```
<Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
ID="id918dbd78b23e4d55b004950c521ea50f" IssueInstant="2018-06-15T03:39:22.032Z"
Version="2.0">
    <Issuer>https://saml.adgangsstyring.eksterntest-
stoettesystemerne.dk</Issuer>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
```

```
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
     <Reference URI="#id918dbd78b23e4d55b004950c521ea50f">
     <Transforms>
     <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
     <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
     </Transforms>
     <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<DigestValue>edQ6UwfGY9bokqHHR+amfOxxourOrZ310OYe8sCxQXs=</DigestValue>
            </Reference>
        </SignedInfo>

<SignatureValue>Ia6CXM3AylDa9zRWFBp96JUBPAIvStNLgm+SoWUFqcY0oacpaOYBBo4dHZAgGqbr
i6FsTCNHJpVIi8gVPr0rSNMCdCR+d2ApM0nknG6aYPqAElmGStWGoR57YPNbZNSp0wGepJD1YMGGCqqy
SF1GRQi/woNhY/yiDNSFasrYbS/klSQa/xtlH80xTI4zNrm9Z+LUQSY9c177CulmYCvNsQ3FQDNZEzXH
3qxBkrtYMGA2K1E/qpk0iQMZB7H0NPGT3YlXAjkGPvwC0XlI+oEBNS3Ai2vk6L07H1MYDMVQeP2c684s
lKm+rACis/GO1oWB9RFGugUgic5o4XB5gt3HQw==</SignatureValue>
        <KeyInfo>
            <X509Data>

<X509Certificate>MIIGHzCCBQegAwIBAgIEUxBEhTANBgkqhkiG9w0BAQsFADBHMQswCQYDVQQGEwJ
ESzESMBAGA1UECgwJVFJVU1QyNDA4MSQwIgYDVQQDDBtUUlVTVDI0MDggU3lzdGVtdGVzdCBYSVggQ0E
wHhcNMTUxMDI4MDY1NDMyWhcNMTgxMDI4MDY1MzU2WjCBjTELMAkGA1UEBhMCREsxIzAhBgNVBAoMGkt
PTUJJVCBBL1MgLy8gQ1ZSOjE5NDM1MDc1MVkwIAYDVQQFExlDVlI6MTk0MzUwNzUtRklEOjUwOTcwMzk
5MDUGA1UEAwwuS09NQklUIFN0w7h0dGVzeXN0ZW1lci1UIChmdW5rdGlvbnNjZXJ0aWZpa2F0KTCCASI
wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIuioynjsh/kimXdOYiYyxJANHhsp6k9GCzc0NgR0mn
D3hyofVObCizG3irBRisY4Xn6NXBaEDz4oR5QUa7g/f3tI4Z5Zl23egczOh3pur4kOjnpAjuKjrLnLdg
2WJadZsydUC69uwyhZNjQS9RLZ90wPWAOINwQzjN/w4s4AA6Vn4JpLdoGU//hiAzMzZDn+ylYZUmiaDt
SuNpE4Roh8Y742rpdAoW6NZIRp5Jg1XRSJNMnYOb0Sy3wu0YCh7eyq4AB/5p6Qwl6xMpr3TZbQKO9rXw
5ZpuCLhnCWtaZehI/iBZBBykwEu+1W/BuPu7xBT8S4O+2CQufPbD8Pr6tbJ8CAwEAAaOCAsowggLGMA4
GA1UdDwEB/wQEAwIDuDCBlwYIKwYBBQUHAQEEgYowgYcwPAYIKwYBBQUHMAGGMGh0dHA6Ly9vY3NwLnN
5c3RlbXRlc3QxOS50cnVzdDI0MDguY29tL3Jlc3BvbmRlcjBHBggrBgEFBQcwAoY7aHR0cDovL2YuYWl
hLnN5c3RlbXRlc3QxOS50cnVzdDI0MDguY29tL3N5c3RlbXRlc3QxOS1jYS5jZXIwggEgBgNVHSAEggE
XMIIBEzCCAQ8GDSsGAQQBgfRRAgQGBAIwgf0wLwYIKwYBBQUHAgEWI2h0dHA6Ly93d3cudHJ1c3QyNDA
4LmNvbS9yZXBvc2l0b3J5MIHJBggrBgEFBQcCAjCBvDAMFgVEYW5JRDADAgEBGoGrRGFuSUQgdGVzdCB
jZXJ0aWZpa2F0ZXIgZnJhIGRlbm5lIENBIHVkc3RlZGVzIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTM
xMy4yLjQuNi40LjIuIERhbklEIHRlc3QgY2VydGlmaWNhdGVzIGZyb20gdGhpcyBDQSBhcmUgaXNzdWV
kIHVuZGVyIE9JRCAxLjMuNi4xLjQuMS4zMTMxMy4yLjQuNi40LjIuMIGqBgNVHR8EgaIwgZ8wPKA6oDi
GNmh0dHA6Ly9jcmwuc3lzdGVtdGVzdDE5LnRydXN0MjQwOC5jb20vc3lzdGVtdGVzdDE5LmNybDBfoF2
gW6RZMFcxCzAJBgNVBAYTAkRLMRIwEAYDVQQKDAlUUlVTVDI0MDgxJDAiBgNVBAMMG1RSVVNUMjQwOCB
TeXN0ZW10ZXN0IFhJWCBDQTEOMAwGA1UEAwwFQ1JMNDQwHwYDVR0jBBgwFoAUzAJVDOSBdK8gVNURFFe
ckVI4f6AwHQYDVR0OBBYEFCQbh/pb3R7yKQytvLeA5XEOFVxjMAkGA1UdEwQCMAAwDQYJKoZIhvcNAQE
LBQADggEBACoRkbV6V45GX5uXmtZzFTSc/ycRD3CoPSfTqCQUR3cMWBE/ERJ8b+0b8K51hsEyK7NSGPT
xz158NbtPd+g2HqRmXOhOvchbzVRonudDb2vuaa4k5CxhUhzXockPNo6phwhf11NMROcSFKMyq+s/Sf4
lQMA3GKe9KofGhDi2DCAAtVGz9nBHIAEQW+Tvj8IYYQ4wKVvfBGp02lWNCEmepRGZkdOBnLHNtis39uY
ezrnMpXuw9nznO7km5408eG928HfcNNHg9omuGhG/y5axGYMM5La1C9dNRAC0JMTiULBfHMVAlMzm8WM
gSk4mof5/VcbRmE2AHJ0wNricpzzAxpg=</X509Certificate>
            </X509Data>
        </KeyInfo>
    </Signature>
    <Subject>
        <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">C=DK,O=19435075,CN=Test Testesen,Serial=74c08b2b-212b-
4f6d-9ce6-0fba1651087d</NameID>
        <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
```

```
<SubjectConfirmationData InResponseTo="a245fg76882j734a25eh6ggfij27ebh"
NotOnOrAfter="2018-06-15T03:44:22.032Z" Recipient="https://demo-
brugervendtsystem.kombit.dk/test/saml/SSO"/>
        </SubjectConfirmation>
    </Subject>
    <Conditions NotBefore="2018-06-15T03:39:22.032Z" NotOnOrAfter="2018-06-
15T03:44:22.032Z">
        <AudienceRestriction>
            <Audience>https://saml.demo-
brugervendtsystem.kombit.dk/test</Audience>
        </AudienceRestriction>
    </Conditions>
    <AuthnStatement AuthnInstant="2018-06-15T03:39:22.032Z"
SessionIndex="1028425489">
    </AuthnStatement>
    <AttributeStatement>
        <Attribute Name="dk:gov:saml:attribute:CvrNumberIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <AttributeValue>19435075</AttributeValue>
        </Attribute>
        <Attribute Name="dk:gov:saml:attribute:SpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <AttributeValue>DK-SAML-2.0</AttributeValue>
        </Attribute>
        <Attribute Name="dk:gov:saml:attribute:KombitSpecVer"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <AttributeValue>1.0</AttributeValue>
        </Attribute>
        <Attribute Name="dk:gov:saml:attribute:AssuranceLevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
            <AttributeValue>4</AttributeValue>
        </Attribute>
        <Attribute Name="dk:gov:saml:attribute:Privileges_intermediate"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">

<AttributeValue>PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48YnBwOlByaXZp
bGVnZUxpc3QgeG1sbnM6YnBwPSJodHRwOi8vaXRzdC5kay9vaW9zYW1sL2Jhc2ljX3ByaXZpbGVnZV9w
cm9maWxlIiB4bWxuczp4c2k9Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvWE1MU2NoZW1hLWluc3RhbmNl
Ij48UHJpdmlsZWdlR3JvdXAgU2NvcGU9InVybjpkazpnb3Y6c2FtbDpjdnJOdW1iZXJJZGVudGlmaWVy
OjE5NDM1MDc1Ij48UHJpdmlsZWdlPmh0dHA6Ly9kZW1vLWJydWdlcnZlbmR0c3lzdGVtLmtvbWJpdC5k
ay9yb2xlcy91c2Vyc3lzdGVtcm9sZS9zZV9zYWcvMTwvUHJpdmlsZWdlPjxDb25zdHJhaW50IE5hbWU9
Imh0dHA6Ly9zdHMuZGVtby5kay9jb25zdHJhaW50cy9LTEUvMSI+MTcuMDAuMDA8L0NvbnN0cmFpbnQ+
PC9Qcml2aWxlZ2VHcm91cD48L2JwcDpQcml2aWxlZ2VMaXN0Pg==</AttributeValue>
        </Attribute>
    </AttributeStatement>
</Assertion>
```

## 1.8 Referencer


| | |
|---|---|
| [NIST-standarden] | “Electronic Authentication Guideline”, NIST Special Publication 800-63 Version 1.0.1<br>http://www.csrc.nist.gov/publications/nistpubs/800-63/SP800- 63v6_3_3.pdf |
| [OIOSAML] | “OIO Web SSO Profile V2.1.0”<br>https://digst.dk/it-loesninger/standarder/oiosaml-profiler/ |
| [OIO-BPP] | “OIO Basic Privile Profile V1.0”<br>https://digst.dk/it-loesninger/standarder/oiosaml-profiler/ |
| [OIO_IDT] | “OIO Identity Token Profile V1.0”<br>https://digst.dk/it-loesninger/standarder/oio-identity-based-web-services-12-oio-idws/ |