DIGITALISERINGSSTYRELSEN

Snitfladespecifikation for tjenester

16. marts 2022
DIGST

Dette dokument indeholder en SAML snitfladespecifikation for den grænseflade, som eID-gateway udstiller mod danske tjenester.

Indhold

1. Indledning

Dette dokument indeholder en SAML snitfladespecifikation for den grænseflade, som eID-gateway udstiller mod danske tjenester.

Snitfladen er baseret på OIOSAML profilen, som et meget stort antal danske myndigheder kender i forvejen fra deres integration til NemLog-in. Formålet med specifikationen er:

a) Tidligt at beskrive snitfladen (*contract first*), så myndigheder kan begynde at vurdere deres integrationsopgave.
b) Lægge snitfladen tæt op ad OIOSAML profilen, så der introduceres få ændringer for myndigheder.
c) Sikre at Digitaliseringsstyrelsens eID-gateways forskellige miljøer udstiller samme snitflade - blot med forskellige endpoints og certifikater således, at myndigheders test- og integrationsarbejde kan starte på eID-gateways integrationstestmiljø og herefter smidigt skifte til produktionsmiljøet.

2. SAML snitfladespecifikation

Med mindre andet angives eksplicit gælder kravene fra OIOSAML 2.0.9 profilen[1] og dernæst SAML 2.0. De vigtigste krav som følger af OIOSAML er gentaget nedenfor af hensyn til overblikket, men læseren gøres opmærksom på, at ikke alle krav er gengivet. Krav som følger direkte af OIOSAML er markeret med blå skrift, så de er lette at skelne.

Nøgleordene "SKAL", "SKAL IKKE", "KRÆVET", "MÅ", "BØR" mv. i dette dokument skal fortolkes som beskrevet i [RFC2119][2].

Tjenesteudbyders request

eID-gateway afviser request fra tjenester, som ikke overholder flg. krav:

- SAML `<AuthnRequest>` SKAL signeres som i OIOSAML.
- Request SKAL have en unik ID og tidsstemples korrekt (IssueInstant).
- HTTP Redirect binding SKAL anvendes over TLS.
- Attributten `urn:oasis:names:tc:SAML:2.0:status:IsPassive` SKAL IKKE anvendes.

eID gatewayens svar

- eID-gateway SKAL anvende HTTP POST over TLS i sit svar.
- I valg af SP location SKAL anvendes værdier fra registrerede metadata.
- Response BØR ikke være signeret.
- Assertion SKAL være signeret og krypteret.
- Kun succesfulde kald MÅ returnere en Assertion og i givet fald højst en.
- <Issuer> elementet SKAL indeholde en unik ID på eID-gateway og dannes på formatet "urn:oasis:names:tc:SAML:2.0:nameid-format:entity".

Afvisning af request

eID-gateway SKAL returnere svar med fejl såfremt et modtaget request ikke kan honoreres. Fejl SKAL indeholde en primær <StatusCode> og BØR indeholde en sekundær <StatusCode> og MÅ indeholde en <StatusMessage>. Nedenfor vises et eksempel på et <Status> element i et svar med fejl:

```
<samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Requester">
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported"/>
  </samlp:StatusCode>
  <samlp:StatusMessage>Yderligere information</samlp:StatusMessage>
```

[1] https://digitaliser.dk/resource/2377872
[2] https://www.ietf.org/rfc/rfc2119.txt

```
</samlp:Status>
```

Tabellen nedenfor angiver hvilke fejl eID-gateway SKAL returnere:

Returneret <Status>	Fejlbeskrivelse
• Primær statuskode: Requester • Sekundær statuskode: RequestDenied	Request afvises pga. fejl af sikkerhedsmæssig karakter, for eksempel: signatur mangler, signatur algoritme mangler, ej understøttet signatur algoritme anvendt, certifikat registreret for dansk tjeneste i eID-gateway kan ikke verificere signatur etc.
• Primær statuskode: VersionMismatch	Request afvises pga. forkert angivelse af værdi for AuthnRequest "Version" attributten
• Primær statuskode: Requester • Sekundær statuskode: NoPassive	Request afvises pga. AuthnRequest "IsPassive" attributten er angivet med "true"
• Primær statuskode: Requester • Sekundær statuskode: RequestDenied • Status message: "Invalid AuthnRequest destination"	Request afvises pga. AuthnRequest "Destination" attributten er angivet med værdi der ikke svarer til eID-gateways "SingleSignOnService" lokation (endpoint)
• Primær statuskode: Requester • Sekundær statuskode: RequestUnsupported • Status message: "Unsupported use of AuthnRequest attribute " + [Attribut]	Request afvises pga. AuthnRequest er angivet med attribut der ikke er understøttet af eID-gateway. I fejlmeddelelse angives hvilken attribut.
• Primær statuskode: Requester • Sekundær statuskode: RequestUnsupported • Status message: "Unsupported use of request element " + [Element]	Request afvises pga. AuthnRequest er angivet med element der ikke er understøttet af eID-gateway. I fejlmeddelelse angives hvilket element.

Indhold af Assertion i svar

`<Subject>` elementet SKAL bevare `NameID` værdi og Format i henhold til de modtagne værdier fra den udenlandske eIDAS Service eller tyske Middleware, men OIOSAML SKAL følges for øvrige aspekter.

Der SKAL højst være et `<AttributeStatement>` element i Assertion.

`<AuthenticationStatement>` elementet skal indeholde et indlejret `<AuthnContext>` element, som kopierer eIDAS LoA værdien direkte til udgående Assertion som fx:

```
<saml2:AuthnContext>

<saml2:AuthnContextClassRef>http://eidas.europa.eu/LoA/high</saml2:AuthnContextClassRef>

</saml2:AuthnContext>
```

eIDAS attributterne i `<AttributeStatement>` SKAL konverteres en-for-en fra den modtagne Assertion fra den udenlandske eIDAS Service / Middleware efter følgende fremgangsmåde:

- Attributnavne oversættes fra eIDAS efter nedenstående tabel.
- FriendlyName SKAL bevares.
- `NameFormat` attributten på attributter SKAL sættes til `urn:oasis:names:tc:SAML:2.0:attrname-format:basic`
- Indholdet (værdien) af `<AttributeValue>` SKAL bevares men `xsi:type` på `<AttributeValue>` sættes til `xs:string`. Undtaget fra dette er værdien på attributterne `CurrentAddress` samt `LegalPersonAddress`, hvor der sker en yderligere konvertering som beskrevet nedenfor i afsnit 0.
- For eIDAS attributter som anvender *transliteration* (som beskrevet i sektion 2.4 of [eIDAS_Attr]) kopieres kun den ene af de to attributværdier (den Latinske), og værdien som har LatinScript sat til "false" frasorteres.

eIDAS Attribut (Natural Person)	DK Attribut
http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier	dk:gov:saml:attribute:eidas:naturalperson:PersonIdentifier
http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName	dk:gov:saml:attribute:eidas:naturalperson:CurrentFamilyName
http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName	dk:gov:saml:attribute:eidas:naturalperson:CurrentGivenName
http://eidas.europa.eu/attributes/naturalperson/DateOfBirth	dk:gov:saml:attribute:eidas:naturalperson:DateOfBirth
http://eidas.europa.eu/attributes/naturalperson/BirthName	dk:gov:saml:attribute:eidas:naturalperson:BirthName
http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth	dk:gov:saml:attribute:eidas:naturalperson:PlaceOfBirth
http://eidas.europa.eu/attributes/naturalperson/CurrentAddress	dk:gov:saml:attribute:eidas:naturalperson:CurrentAddress
http://eidas.europa.eu/attributes/naturalperson/Gender	dk:gov:saml:attribute:eidas:naturalperson:Gender

eIDAS Attribut (Legal Person)	DK Attribut
http://eidas.europa.eu/attributes/legalperson/LegalPersonIdentifier	dk:gov:saml:attribute:eidas:legalperson:LegalPersonIdentifier
http://eidas.europa.eu/attributes/legalperson/LegalName	dk:gov:saml:attribute:eidas:legalperson:LegalName
http://eidas.europa.eu/attributes/legalperson/LegalPersonAddress	dk:gov:saml:attribute:eidas:legalperson:LegalPersonAddress
http://eidas.europa.eu/attributes/legalperson/VATRegistrationNumber	dk:gov:saml:attribute:eidas:legalperson:VATRegistrationNumber
http://eidas.europa.eu/attributes/legalperson/TaxReference	dk:gov:saml:attribute:eidas:legalperson:TaxReference
http://eidas.europa.eu/attributes/legalperson/D-2012-17-EUIdentifier	dk:gov:saml:attribute:eidas:legalperson:D-2012-17-EUIdentifier
http://eidas.europa.eu/attributes/legalperson/LEI	dk:gov:saml:attribute:eidas:legalperson:LEI
http://eidas.europa.eu/attributes/legalperson/EORI	dk:gov:saml:attribute:eidas:legalperson:EORI
http://eidas.europa.eu/attributes/legalperson/SEED	dk:gov:saml:attribute:eidas:legalperson:SEED
http://eidas.europa.eu/attributes/legalperson/SIC	dk:gov:saml:attribute:eidas:legalperson:SIC

Bemærk at en SAML Assertion jævnfør eIDAS både kan indeholde attributter fra en 'NaturalPerson' og 'LegalPerson' på samme tid, og dette skal direkte reflekteres i den vekslede 'DK' Assertion.

Assertion SKAL indeholde et `<AudienceRestriction>` element, som specificerer EntityID for den tjeneste, der anmodede om autentifikation.

`<AttributeStatement>` KAN indeholde øvrige attributter som specificeret i OIOSAML, der er beriget af eIDgateway.

Konvertering af attributterne CurrentAddress og LegalPersonAddress
eIDAS attributten `CurrentAddress` er defineret i sektionerne 2.2.9 af [eIDAS_Attr]. Værdien er en Base64-indkodning af en XML struktur af typen `CurrentAddressStructuredType`:

```
<xsd:complexType name="CurrentAddressStructuredType">
  <xsd:annotation>
    <xsd:documentation>
```

```
      Current address of the natural person.
    </xsd:documentation>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="PoBox" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="LocatorDesignator" type="xsd:string" minOccurs="0" max-
Occurs="1"/>
    <xsd:element name="LocatorName" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="CvaddressArea" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="Thoroughfare" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="PostName" type="xsd:string" minOccurs="0" maxOccurs="1"/>
    <xsd:element name="AdminunitFirstline" type="xsd:string" minOccurs="0" max-
Occurs="1"/>
    <xsd:element name="AdminunitSecondline" type="xsd:string" minOccurs="0" max-
Occurs="1"/>
    <xsd:element name="PostCode" type="xsd:string" minOccurs="0" maxOccurs="1"/>
  </xsd:sequence>
</xsd:complexType>
```

Et eksempel på en instans af ovenstående struktur kunne være:

```
<saml2:Attribute xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                           FriendlyName="CurrentAddress"
                           Name="http://eidas.europa.eu/attributes/naturalperson/Cur-
rentAddress"
                           NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-for-
mat:uri">
  <saml2:AttributeValue xsi:type="eidas:CurrentAddressType">
    PGVpZGFzOkxvY2F0b3JEZXNpZ25hdG9yPjIyPC9laWRhczpMb2NhdG9yRGVzaWduYX
    Rvcj48ZWlkYXM6VGhvcm91Z2hmYXJlPkFyY2FjaWEgQXZlbnVlPC9laWRhczpUaG9y
    b3VnaGZhcmU+DQo8ZWlkYXM6UG9zdE5hbWU+TG9uZG9uPC9laWRhczpQb3N0TmFtZT
    4NCjxlaWRhczpQb3N0Q29kZT5TVzFBIDFBQTwvZWlkYXM6UG9zdENvZGU+
  </saml2:AttributeValue>
</saml2:Attribute>
```

Attributværdien udgør en Base64 indkodning af følgende XML-brudstykke:

```
<eidas:LocatorDesignator>22</eidas:LocatorDesignator>
<eidas:Thoroughfare>Arcacia Avenue</eidas:Thoroughfare>
<eidas:PostName>London</eidas:PostName>
<eidas:PostCode>SW1A 1AA</eidas:Postcode>
```

En sådan struktur er ikke let at behandle for standard SAML software, og der defineres derfor en ny `eidasNaturalPersonAddress` attribut (`dk:gov:saml:attribute:eidas:naturalperson:CurrentAddress`), som der konverteres til.

Attributten `eidasNaturalPersonAddress` defineres til at være en ikke-tom attribut indeholdende key/value par adskilt med semikolon. Nøgleelementerne er navnene på elementerne i `CurrentAddressStructuredType` og værdielementerne er de tilhørende værdier. Nøgler og værdier i hvert par adskilles med et '=' tegn og både nøgler og værdier SKAL være URL-indkodede.

eIDAS-attributten `CurrentAddress` ovenfor vil dermed blive konverteret til nedenstående attribut:

```
<saml2:Attribute xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
                            FriendlyName="eidasNaturalPersonAddress"
                            Name="dk:gov:saml:attribute:eidas:naturalperson:CurrentAddress" "
                            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-for-
mat:uri">
  <saml2:AttributeValue xsi:type="xs:string">
    LocatorDesignator=22;Thoroughfare=Arcacia%20Avenue;PostName=London;Post-
Code=SW1A%201AA
  </saml2:AttributeValue>
</saml2:Attribute>
```

Tilsvarende indkodningsregler gælder for attributten `LegalPersonAddress`. Denne har på samme måde defineret sin egen type (`LegalPersonAddressStructured-Type`) i eIDAS skemaet, og den resulterende DK attribut dannes analogt som key/value par adskilt med '=' tegn og URL-indkodning.

Håndtering af repræsentanter
eIDAS specifikationen [eIDAS_Attr] beskriver i afsnit 2.8, hvorledes repræsentanter for en juridisk eller fysisk person kan håndteres. En repræsentant angives her ved at genanvende de eksisterende eIDAS attributter, hvor attributnavnet blot tilføjes et "`representative`" dvs. der anvendes flg. prefixes i navnet:

- `http://eidas.europa.eu/attributes/naturalperson/representative/`
- `http://eidas.europa.eu/attributes/legalperson/representative/`

I snitfladen mod danske tjenester konverteres dette på flg. måde:

Attributtens navn SKAL dannes ved at tilføje et "`representative`" før sidste del af attributnavnet dvs. `http://eidas.europa.eu/attributes/naturalperson/representative/PersonIdentifier`

bliver til

```
dk:gov:saml:attribute:eidas:naturalperson:representative:PersonIdentifier
```

Attributtens værdi SKAL indkodes på samme måde som beskrevet tidligere i denne specifikation, således at attributværdien indkodes på samme måde uanset om der er tale om en repræsentant eller ej.

Algoritmer

- Gatewayen SKAL anvende SHA-256 som hashfunktion og RSA som signaturalgoritme (alle varianter accepteres).
- Indgående SKAL acceptere SHA-256 (SHA2) for tjenesteudbydernes del.

Logout

SAML Single Logout Profile understøttes ikke mod danske tjenester, men alene i integrationen mod NemLog-in som SAML Service Provider. Danske tjenester kan med andre ord ikke forvente et Single Logout Endpoint på eID-gateway.

Identity Provider Discovery Profile

Denne profil understøttes ikke af eID-gateway som Identity Provider.

Attribute Query profile

Denne profil understøttes ikke af eID-gateway som Identity Provider.

Persistent Pseudonym profile

Denne profil understøttes ikke af eID-gateway som Identity Provider.

Metadata

eID-gateway SKAL kunne modtage gyldige metadatafiler for danske tjenester og skal tilsvarende udstille en SAML metadatafil i rollen som SAML Identity Provider.

Usignerede metadatafiler fra tjenesteudbydere SKAL modtages af eID-gateway.

3. Referencer

[OIOSAML 2.0.9]	"OIOSAML Web SSO Profile, 2.0.9, Digitaliseringsstyrelsen". https://digitaliser.dk/resource/2377872
[eIDAS_Attr]	"eIDAS SAML Attribute Profile". https://ec.europa.eu/cefdigital/wiki/download/attachments/82773108/eIDAS%20SAML%20Attribute%20Profile%20v1.2%20Final.pdf

4. Ændringslog

Date	Version	Beskrivelse af ændring	Initialer
2018-15-02	1.	Dokument oprettet	DIGST
2022-16-03	1.1	Dokumentet er blevet strømlinet, så det ligner det resterende materiale ifm. tilslutning til DK eIDAS Connector. Enkelte tilpasninger i anvendt terminologi.	IDAWI