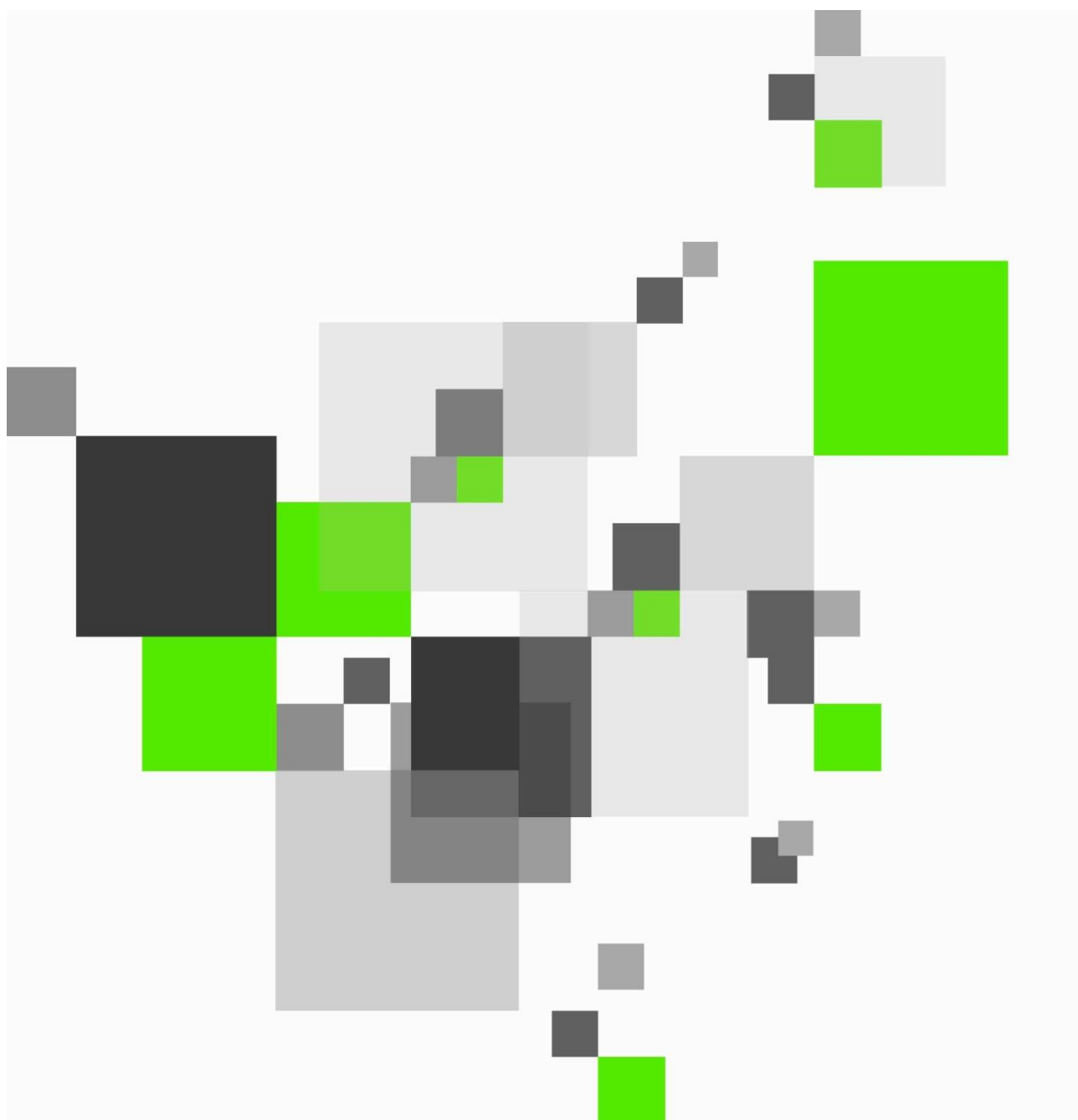


Security Token Service –

Snitflade OIO WS Trust



Indholdsfortegnelse

1.	Versionsnummer	3
2.	Snitfladebeskrivelse	3
3.	Servicebeskrivelse	3
3.1	Identity provider	3
3.2	Supported binding	3
3.3	Signering af request.....	3
3.4	Krav til <RequestSecurityToken>	4
3.5	Input parametre	4
3.6	Output – RSTR Response	5
3.6.1	Binding	6
3.6.2	Signering	6
4.	Teknisk beskrivelse	6
5.	Kommunikation	6
6.	Transformationsmekanismer	7
7.	Eventuelt yderligere oplysninger	7

1. Versionsnummer

Snitfladens version er 1.0.

2. Snitfladebeskrivelse

Dokumentet beskriver en snitflade hvor der kan forespørges om et SAML2.0 token ved brug af en WS-Trust snitflade.

Snitfladen supporteres af Security Token Service støttesystemet.

Snitfladen implementerer OIO WS-Trust Profile v1 0 1 [WST-OIO], og med mindre andet er angivet følges [WST-OIO]. På områder hvor dette dokument er mere specifikt end [WST-OIO], er dette dokument gældende. Hvis der er uoverensstemmelse imellem dette dokument og [WST-OIO], og dette dokument ikke overholder [WST-OIO], så er [WST-OIO] gældende.

Snitfladen understøtter den WS-Trust baserede autentifikations forespørgselsprotokol, hvor en service provider sender et token request til Security Token Service i form af et RequestSecurityToken element (RST), som så behandles af Security Token Service, og et RequestSecurityTokenResponse bliver sendt indeholdende et signeret SAML2.0 assertion tilbage til klienten.

3. Servicebeskrivelse

3.1 Identity provider

Anvendersystemet og Security Token Service SKAL have udvekslet metadata før Security Token Service vil acceptere et RequestSecurityToken fra **anvendersystemet**.

Metadata for servicen er adressen og vil blive uploadet til støttesystem Administrationsmodul og derfra provisioneret til Security Token Service.

Anvendersystemet er identificeret ved et eller flere OCES certifikater.

3.2 Supported binding

Liberty Basic SOAP Binding.

HTTP over TLS SKAL anvendes. Der anvendes IKKE klientcertifikat med TLS.

3.3 Signering af request

Elementet <wst:RequestSecurityToken> SKAL signeres af den der laver forespørgslen.

Der SKAL benyttes det VOCES eller FOCES certifikat der på forhånd er registreret i Administrationsportalen, til at foretage signeringen af RST.

3.4 Krav til <RequestSecurityToken>

Elementet <wst:RequestType> SKAL indikere udstedelses binding og derfor skal følgende URI anvendes: <http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue>.

Elementet <wsp:AppliesTo> SKAL indeholde en <wsa:EndpointReference> der identificerer den web service udbyder eller den specifikke service som identitetstokenet skal udstedes for.

3.5 Inputparametre (RST request element)

Det er nødvendigt for kalderen at "fortælle" STS hvilken Anvenderkontekst som kalderen benytter. Måden dette er implementeret på, er ved at kalderen, i listen med requested claims, tilføjer et claim med en specifik claim type, der angiver den Anvenderkontekst der benyttes.

Parameter	Obligatorisk	Udfaldsrum
HTTP METHOD	*	POST
RequestSecurityToken	*	Forespørgsel for at modtage et Token
RequestType	*	Indikation af "class of function" som bliver forespurgt. Her skal benyttes http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue jf. afsnit 3.4
AppliesTo	*	Specifere scope't som Token'et skal overholde. Jf afsnit 3.4 skal <wsa:EndpointReference> benyttes
TokenType	*	Beskriver typen af sikkerhedstoken'et, specificeret som en URI. Skal sættes til: http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
Claims - Anvenderkontekst	*	Præcist eet ClaimType element i Claims listen, der repræsenterer den Anvenderkontekst der arbejdes i. Claim type skal være: "dk:gov:saml:attribute:CvrNumberIdentifier" og claim value skal være CVR for den benyttede Anvenderkontekst

Eksempel på et RST element:

```
<S11:Envelope xmlns:S11="..." xmlns:wsu="..." xmlns:wsse="..." xmlns:xenc="..."
  xmlns:wst="...">
  <S11:Header>
    <wsa:Action>http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue</wsa:Action>
    <wsa:MessageID>urn:uuid:99999999-0000-0000-...</wsa:MessageID>
    <wsa:To>http://sts.example.org</wsa:To>
    <wsse:Security mustUnderstand="1">
```

```

<wsu:Timestamp wsu:ID="ts"> ... </wsu:Timestamp>
<ds:Signature xmlns:ds="...">
  <ds:SignedInfo> ...
    <ds:Reference URI="#req"> ... </ds:Reference>
    <ds:Reference URI="#ts"> ... </ds:Reference>
    <!-- More references to other header elements -->
  </ds:SignedInfo>
  <ds:SignatureValue> ... </ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data> ... sender certificate ... </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
</wsse:Security>
</S11:Header>
<S11:Body wsu:Id="req">
  <wst:RequestSecurityToken Context="urn:uuid:00000...">
    <wst:TokenType>
      http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0
    </wst:TokenType>
    <wst:RequestType>
      http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
    </wst:RequestType>
    <wsp:AppliesTo>
      <wsa:EndpointReference>
        <wsa:Address>http://agency_x.dk</wsa:Address>
      </wsa:EndpointReference>
    </wsp:AppliesTo>
    <wst:Claims wst:Dialect="http://docs.oasis-open.org/wsfed/authorization/200706/authclaims"
      xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706">
      <auth:ClaimType Uri="dk:gov:saml:attribute:CvrNumberIdentifier" Optional="false">
        <auth:Value>12345678</auth:Value>
      </auth:ClaimType>
    </wst:Claims>
  </wst:RequestSecurityToken>
</S11:Body>
</S11:Envelope>

```

3.6 Output – RSTR Response

Efter brugerauthentifikationen, sendes som svar på det modtagne RST element, et RSTR svar som indeholder præcis eet <RequestSecurityTokenResponseCollection> element med præcis eet <RequestSecurityTokenResponse> element.

Parameter	Obligatorisk	Udfaldsrum
HTTP METHOD	*	POST
RequestSecurityToken-Response	*	<p>Indeholder et RequestedSecurityToken indeholder med SAML2.0 assertion.</p> <p>KOMBIT Attribut Profil v1.0 benyttes.</p> <p>Den udstedte assertion indeholder altid en attribut med brugerens anvenderkontekst. Denne anvenderkontekst modsvarer den anvenderkontekst som kalderen sendte med i RST.</p>

AppliesTo		Indeholder <wsa:EndpointReference> fra forespørgslen
-----------	--	--

3.6 Binding

RSTR returneres ved brug af HTTP POST binding.
Kun HTTP på TLS (HTTPS) tillades.

3.6 Signering

Security Token Service signerer svaret og det udstedte "SAML 2.0 assertion" indeholdende attributter om brugeren.

Det udstedte "assertion" SKAL indeholde et SubjectConfirmation element med en "holder-of-key" reference til forespørgerens nøgle.

3.7 Fejlbeskeder

Hvis der opstår en fejl under behandling af request security token beskeden returneres en SOAP fault besked til kalderen. Denne SOAP fault indeholder en detaljeret besked om fejlen der opstod under behandling af forespørgslen.

Der understøttes følgende fejlkoder:

Fejlkode	Beskrivelse
100	Uventet fejl. Fejl hvor årsagen ikke er kendt.
101	Den anvendte konfiguration kendes ikke. Kalderen forespørger et token for en service STS ikke kender, eller som en kalder STS ikke kender.
103	Forkert formateret forespørgsel. Der er en fejl i forespørgslen.
104	Der forespørges et endpoint der ikke findes.
106	Der opstod en transaktionsfejl under commit af auditlog.
110	Ikke understøttet. Der benyttes en endpoint konfiguration som ikke understøttes.
111	Konfigurationsfejl. Der er en fejl i konfigurationen, der gør at forespørgslen ikke kan behandles.
130	Databasfejl. Der er opstået en fejl ved kommunikation/adgang til den underliggende database.

4. Teknisk beskrivelse

Snitfladen er implementeret i Safewhere*Identify produktet.

5. Kommunikation

Snitfladen anvender HTTPS for at sikre meddelelses fortrolighed og integritet.



6. Transformationsmekanismer

N/A

7. Eventuelt yderligere oplysninger

<http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3.wsd>