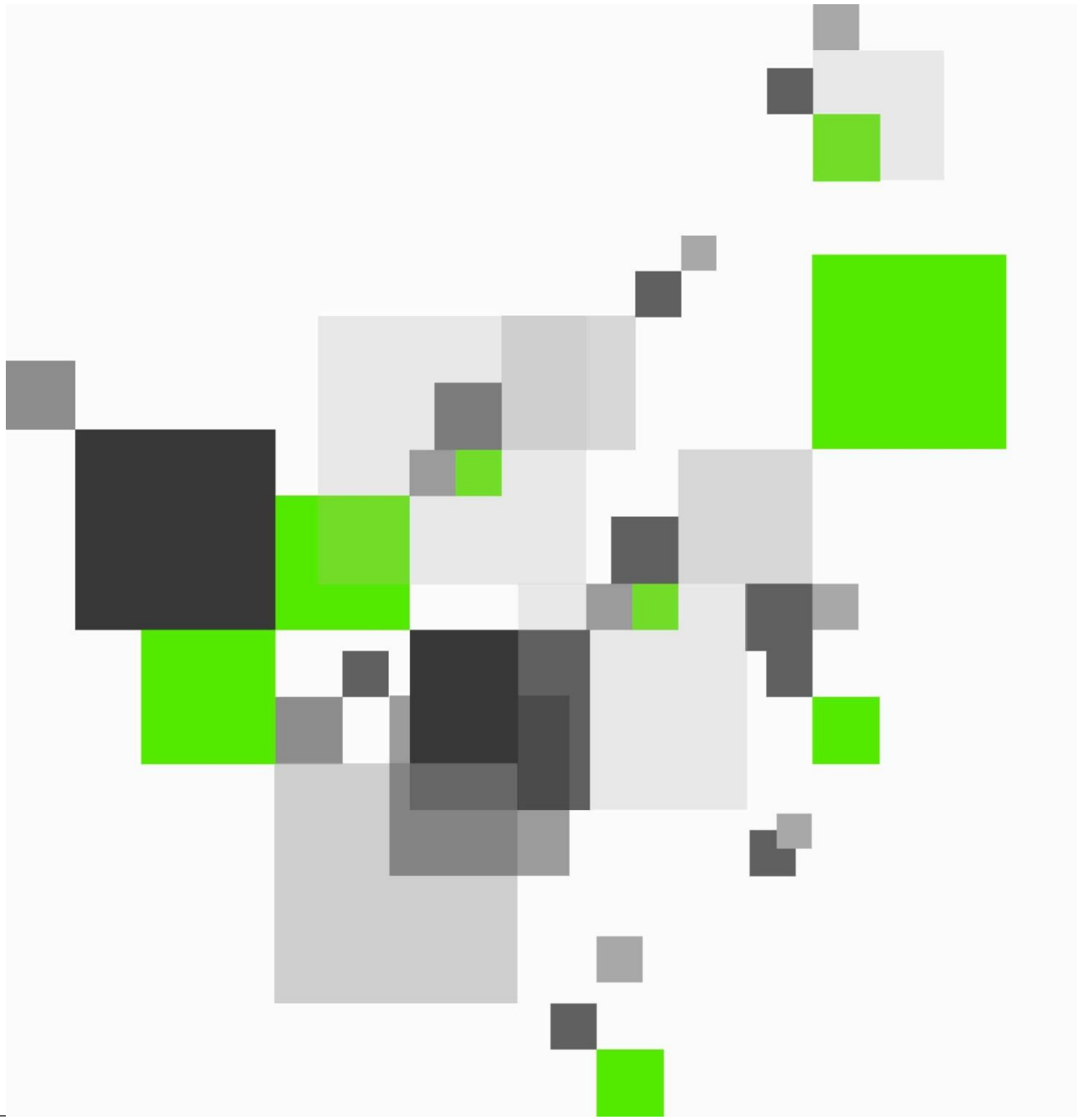
Security Token Service –

Snitflade WS Trust REST Service



Indholdsfortegnelse

1. Versionsnummer

Snitfladens version er 1.0.

2. Snitfladebeskrivelse

Dokumentet beskriver en snitflade hvor man forespørger på tokens ved brug af en REST snitflade, i stedet for den WS-Trust variant som også understøttes.

Snitfladen understøttes af støttesystemet Security Token Service (STS).

Snitfladen efterligner funktionaliteten på standard OIO WS-Trust snitfladen ved at anvende et REST snitflade. Det betyder at der kræves de samme parametre som i en OIO WS-Trust snitflade, men denne snitflade er REST baseret og anvender json til at indkapsle parametre.

Ved brug af snitfladen kan et **anvendersystem** forespørge om et token til at kalde en eksisterende service ved brug af et REST kald og et token bliver så udstede og sendt i et response til REST kaldet.

3. Servicebeskrivelse

Kalderen kalder RST endpoint'et med en json struktur, RequestSecurityToken. Json strukturen bliver sendt med en HTTP POST over TLS.

Security Tolken Service udsteder et nyt SAML 2.0 token og returnerer dette i svaret på REST kaldet.

3.1 Input parametre

Parameter	Required	Structure
HTTP METHOD	*	POST

RequestSecurityToken object	*	RequestSecurityToken: {
		"AppliesTo" : {
		"EndpointReference" : {
		"Address" : {
		"type" : "string"
		}
		}
		},
		"KeyType" : {
		"type" : "string",
		},
		"RequestType" : "http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue"
		"TokenType" : http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile- 1.1#SAMLV2.0
		"Anvenderkontekst" : {

		"type" : "string",
		},
		"OnBehalfOf" : {
		"type" : "string",
		}
		}

3.2 Output

REST snitfladen returnerer en relevant HTTP kode, som angiver status på operationen.

På http 200, returneres der et SAML2 token i json format i http svaret til klienten. Dette token er det samme SAML2 token som ville have været inkluderet i RequestedSecurityToken elementet i RequestSecurityTokenResponse elementet som returneres med WS-Trust.

Det returnerede token bliver signeret med Security Token Servicens tokensignerings certifikat. Det er ikke krypteret til det certifikat for den service, som det var forespurgt fra.

Structure	Code	Message
HTTP Status Code	200 400 401 500 503	OK Bad Request Unauthorized Internal Server Error Service Unavailable

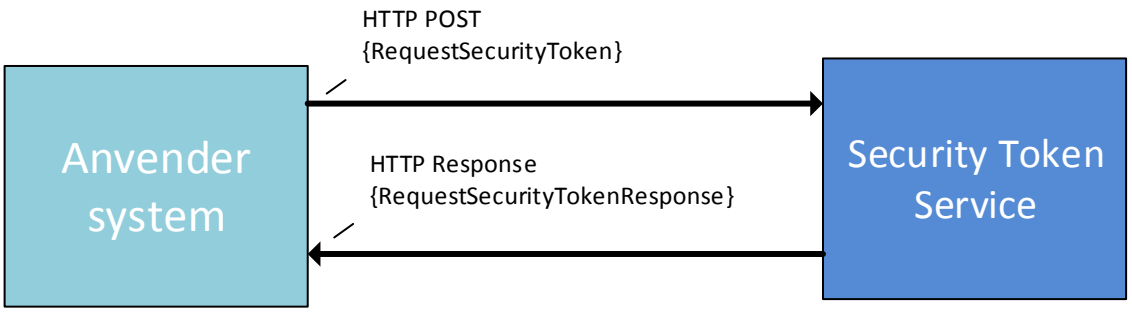
OIOSAML SAML2 token		Base64 encoded text string with the issued SAML2.0 token.
		
		{
		"AppliesTo" : {
		"EndpointReference" : {
		"Address" : {
		"type" : "string"
		}
		}
		},
		"KeyType" : {
		"type" : "string",
		},
		"Lifetime" : {
		"type" : "string",
		},
		"RequestedSecurityToken" : {
		"Assertion" : {
		"type" : "string",
		}
		},
		"RequestType" : "http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue"
		"TokenType" : "http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile- 1.1#SAMLV2.0"
		}

4. Teknisk beskrivelse

Servicen er implementeret som en REST service.

5. Kommunikation

Der benyttes HTTPS over TLS ved kommunikation. Der benyttes klientcertifikat til autentifikation og kalderen skal præsentere et FOCES eller VOCES certifikat ved autentifikation. Certifikatet skal på forhånd være registreret i Administrationsportalen til at kunne kalde servicen.



6. Transformationsmekanismer

N/A

7. Eventuelt yderligere oplysninger

STS-REST.json snitfladespecifikation