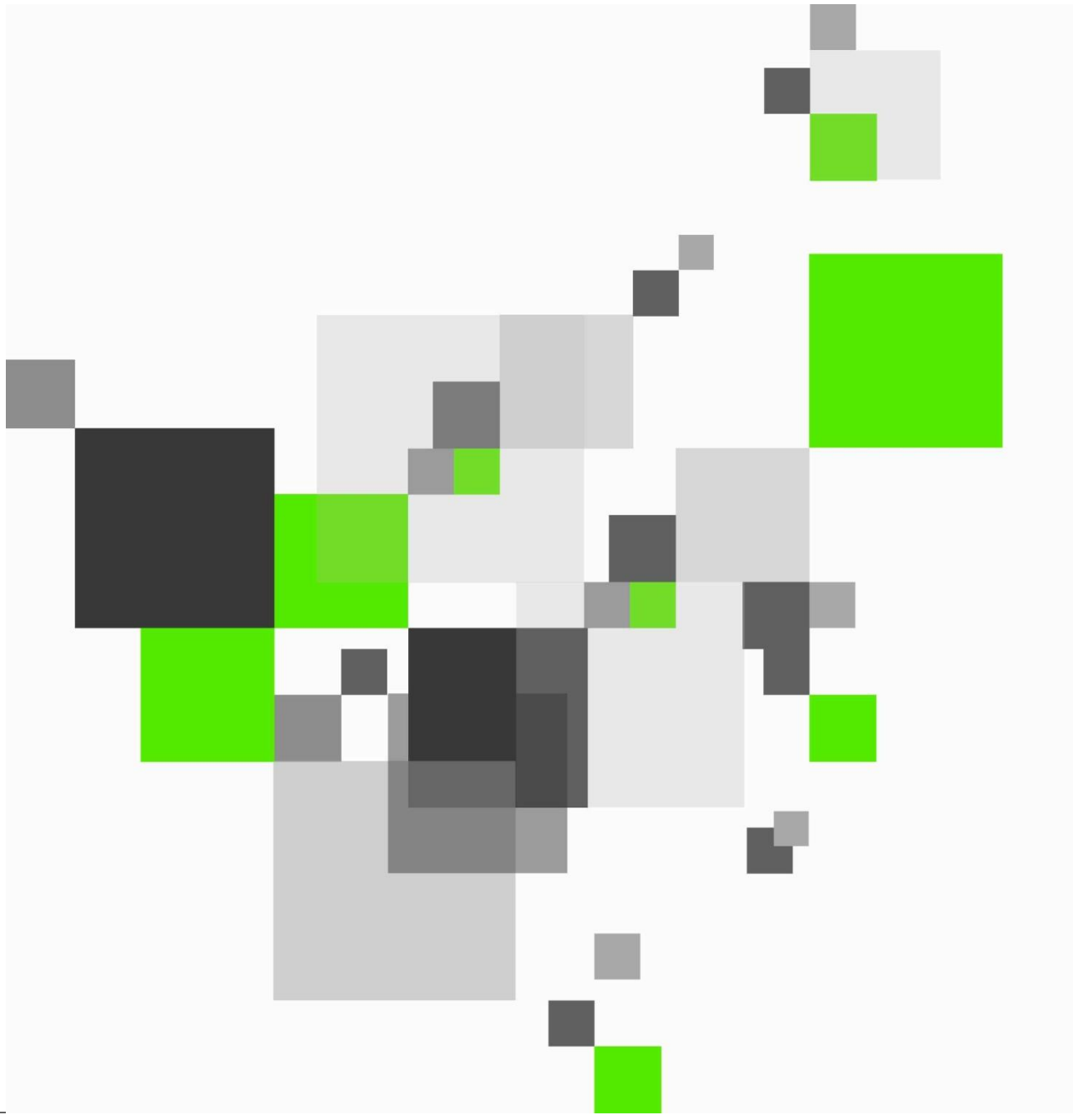
Security Token Service –

Snitflade JWT-token



Indholdsfortegnelse

1. Versionsnummer

Snitfladens version er 1.0.

2. Snitfladebeskrivelse

Dokumentet beskriver en snitflade hvor der kan forespørges om et SAML token ved brug af en JWT (JSON Web Token)- snitflade.

Snitfladen supporteres af Security Token Service støttesystemet.

Snitfladen implementerer ”KOMBIT OAuth Token Request Profile v0.9-”,

Servicen udsteder token i forhold til ”KOMBIT JWT Profile v0.9”,

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 uploaded til støttesystem Administrationsmodul og derfra provisioneret til Security Token Service.

Anvendersystemet er identificeret ved et eller flere OCES certifikater.

3.2 Supported binding

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

3.3 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, giver et client-id og et scope, der benyttes.

Parameter	Obligatorisk	Udfaldsrum
HTTP METHOD	*	POST

client_id	*	Navn på en provisioneret service
grant_type	*	Skal være client_credentials
scope	*	Skal indeholde EntityId og Anvenderkontekst

Eksempel på et RST element:

```
POST /token HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded

Endpoint : https:// n2adgangsstyring.stoettesystemerne.dk/runtime/api/rest/oauth/v1/issue


client_id=https%3A%2F%2Flocalhost%3A44302%2Fkombit%2Fservice
&grant_type=client_credentials
&scope=entityid%3Ahttps%3A%2F%2Flocalhost%3A44302%2Fkombit%2Fservice
%2Canvenderkontekst%3A12345678
```

3.4 Output – RSTR Response

Efter brugerautentifikationen, sendes som svar på det modtagne RST element, et RSTR svar som indeholder flg. elementer:

Parameter	Obligatorisk	Udfaldsrum
HTTP METHOD	*	POST
Acess-token	*	Selve token
Token-type	*	Typen på det udstedte token, holder-Of-Key.
Expires-in	*	Levetid på token i sekunder

3.6 Binding

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

3.6 Endpoints

Endpoint for ekstern test: https://n2adgangsstyring.eksterntest-stoettesystemerne.dk/runtime/api/rest/oauth/v1/issue?

Endpoint for produktion:
https://n2adgangsstyring.stoettesystemerne.dk/runtime/api/rest/oauth/v1/issue

3.7 Fejlbeskeder

Hvis der opstår en fejl under behandling af request jwt token beskeden returneres en besked til kalderen. Denne besked 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	Databasefejl. Der er opstået en fejl ved kommunikation/adgang til den underliggende database.

4. Teknisk beskrivelse

Snitfladen er implementeret i Safewhere*Identify produktet.

5. Bilag

VA-214_Bilag_2_KOMBIT_JWT_Profile_0.9_.p

VA-214_Bilag_1_KOMBIT_OAuth_Token_Req