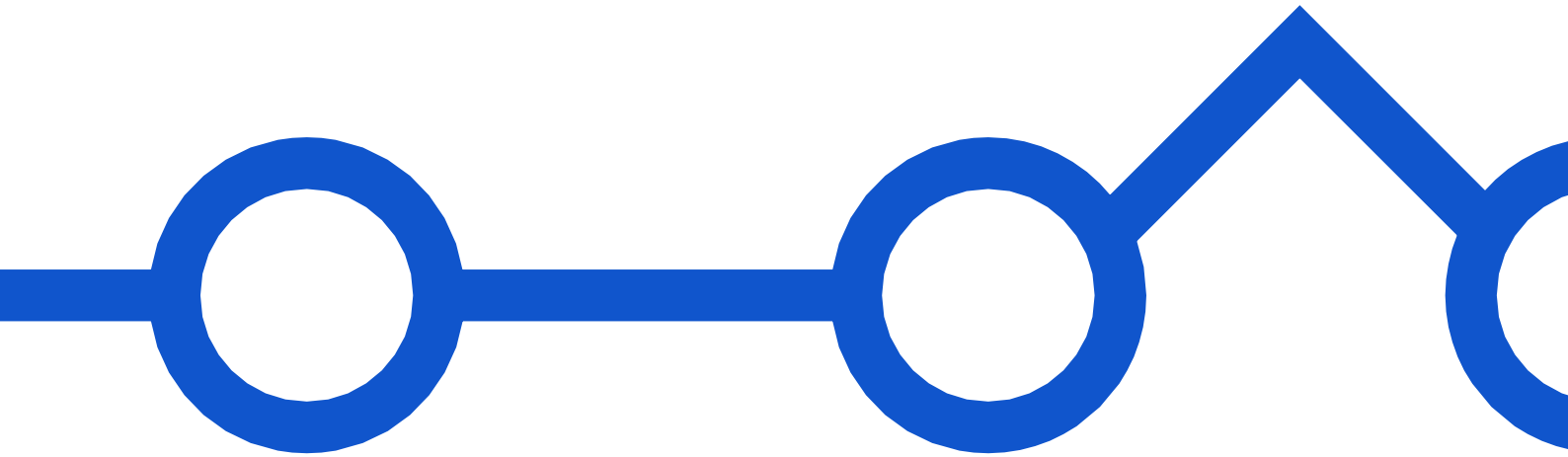
DIGITALISERINGS KATALOGET

SF1516 SIKKERHED – HENT ACCESS TOKEN

Integrationsversion 1.0



KOMBIT
Kommunernes it-fællesskab

KDI – Kommunernes Data og Infrastruktur
Integrationsbeskrivelsen er senest opdateret: *2021.08.25*

VERSIONSHISTORIK

Integrationen er versioneret med et versionsnummer bestående af en hovedversion med tilhørende underversion. En underversion er altid bagud kompatibel.

Integrationsbeskrivelsen kan ændres uden, at det medfører ændring af integrationens versionsnummer, fx ved præciseringer i teksten.

Integrationsversion	Dato	Kommentar
1.0	2021-10-11	Første version
1.0	2021-08-10	Udkast

INDHOLD

LÆSEVEJLEDNING

En integration består af en eller flere services. Dokumentationen for en integration er sammensat af en integrationsbeskrivelse, en eller flere servicebeskrivelser, samt eventuelle bilag.

Integrationsbeskrivelsen er målrettet kommuner og leverandører af it-løsninger til kommunerne, og har sit udgangspunkt i forretningen. Den beskriver formål og kontekst for integrationen suppleret med konkrete forretningsmæssige anvisninger.

Nedenfor kan du læse om hvilke kapitler i integrationsbeskrivelsen, der er mest relevant for din målgruppe:

- Forretning (er primært henvendt til kommunernes digitaliseringskonsulenter, projektledere, it-arkitekter mfl.): Læs kapitel 1 og 5-6.
- Udvikling og test (er primært henvendt til kommunens leverandør, it-arkitekter og udviklere mfl.): Læs kapitel 2-5
- Drift (er primært henvendt til kommunens leverandør, kommunens driftsansvarlige mfl.): Læs kapitel 3 og 5

Den funktionelle beskrivelse af de services, som er tilknyttet integrationen, finder du i de tilhørende servicebeskrivelser.

BEGREBER

Anvendersystem: Er en fællesbetegnelse for et Modtager- og Afsendersystem.

Fælleskommunal infrastruktur: En infrastruktur af standarder og tekniske løsninger, som gør det muligt for kommunerne at udveksle data og udføre operationer på tværs af myndigheder og it-systemer.

Serviceplatformen: Serviceplatformen er en integrationsplatform, der udstiller data og funktionalitet fra forskellige fag- og kildesystemer som services til brug for kommunernes it-løsninger.

Serviceudbydersystem: Det it-system, der udstiller en service.

1. OVERORDNET BESKRIVELSE

I dette kapitel beskrives anvendelsen af integrationen ud fra et forretningsperspektiv. Formålet med kapitlet er at sætte anvendere i stand til at vurdere, om denne integration opfylder deres forretningsmæssige behov.

1.1. Integrationens forretningsmæssige formål

Integrationen giver kommunale fagsystemer mulighed for at få vekslet et SAML Token, udstedt af Security Token Service, til et Access Token.

Access Token skal bruges i fagsystemets kald til de RESTful webservices på Serviceplatformen, der accepterer Access Tokens.

Hvis denne integration benyttes af et eller flere KOMBIT-anvendersystem(er), fremgår det forretningsmæssige formål for deres brug af denne oversigt.

Introduktion til forretningsunderstøttelse
Dette afsnit indeholder en overordnet beskrivelse af den forretning, som integrationen understøtter.

Integrationen understøtter Digitaliseringsstyrelsens OIOIDWS-profil for brug af tokenveksling ved kald af en RESTful webservice på Serviceplatformen.

Ved kald af tokenveksler, skal man præsentere et SAML-token (dannet som beskrevet i SF1514 Sikkerhed - Hent Token fra Security Token Service). Som svar fra servicen får man et kortere Access Token. Dette Access Token kan derefter bruges inden for et specifikt timeout til kald af de egentlige RESTful webservices, som understøtter denne kaldsmodel.

Integrationen indeholder desuden en demoservice, der kan bruges til at afprøve Access Token-kaldsmodellen.Integrationen understøtter forretningen med:

Integrationen indgår som en del af forretningsområdet ”Adgangsstyring”.

1.2. Brug af referencedata

Integrationen er ikke afhængig af referencedata.

1.3. Opgradering fra tidligere version

Dette er første version af integrationen.

2. BESKRIVELSE AF INTEGRATIONENS SERVICES

Dette kapitel beskriver de services, som indgår i integrationen, herunder også eksempler på integrationsmønstre, hvor flere af integrationens services indgår. Dette er imidlertid ikke en udtømmende liste af de mulige anvendelser, som integrationen giver.

2.1. Integrationsmønstre

Integrationen tilbyder to webservices af typen RESTful webservice.

2.2. Forretningsflow

Dette afsnit giver en overordnet introduktion til de services, som indgår i integrationen, samt sammenhæng. En detaljeret beskrivelse af de enkelte services findes i de tilhørende Servicebeskrivelser.

RESTful web services er ikke i stand til at håndtere SAML-Tokens i kaldsheaderen, da SAML-Tokens er større end størrelsesbegrænsningerne på http-headers. Derfor har Digitaliseringsstyrelsen, som en del af deres OIOIDWS-specifikationer, defineret en profil for hvorledes man kan veksle et SAML Token til et mindre Access Token, der kan anvendes i f.eks. en RESTful web services [OIOIDWS]. Denne profil er basis for nærværende løsning.

SAML Token hentes med den eksisterende service Security Token Service, som beskrevet i SF1514.

Løsningen bygger på etableringen af en særlig service <*Mediator*>AccessTokenHent på mediatoren – dvs. det system der ønsker at formidle en RESTful service. Dette kunne f.eks. være Serviceplatformen. På Serviceplatformen hedder denne service altså, ”ServiceplatformAccessTokenHent”. Servicen veksler et SAML Token, opnået ved kald af Security Token Service, til et Access Token. Derudover lagrer servicen mapningen fra AccessToken til SAML Token i en Access Token Store på Mediatoren, f.eks. Serviceplatformen.

Med dette Access Token er det muligt at kalde en Kombit RESTful web service.

Kombit RESTful web service vil derefter validere Access Token op imod SAML Token, så det er muligt at verificere om kalder er autoriseret korrekt.

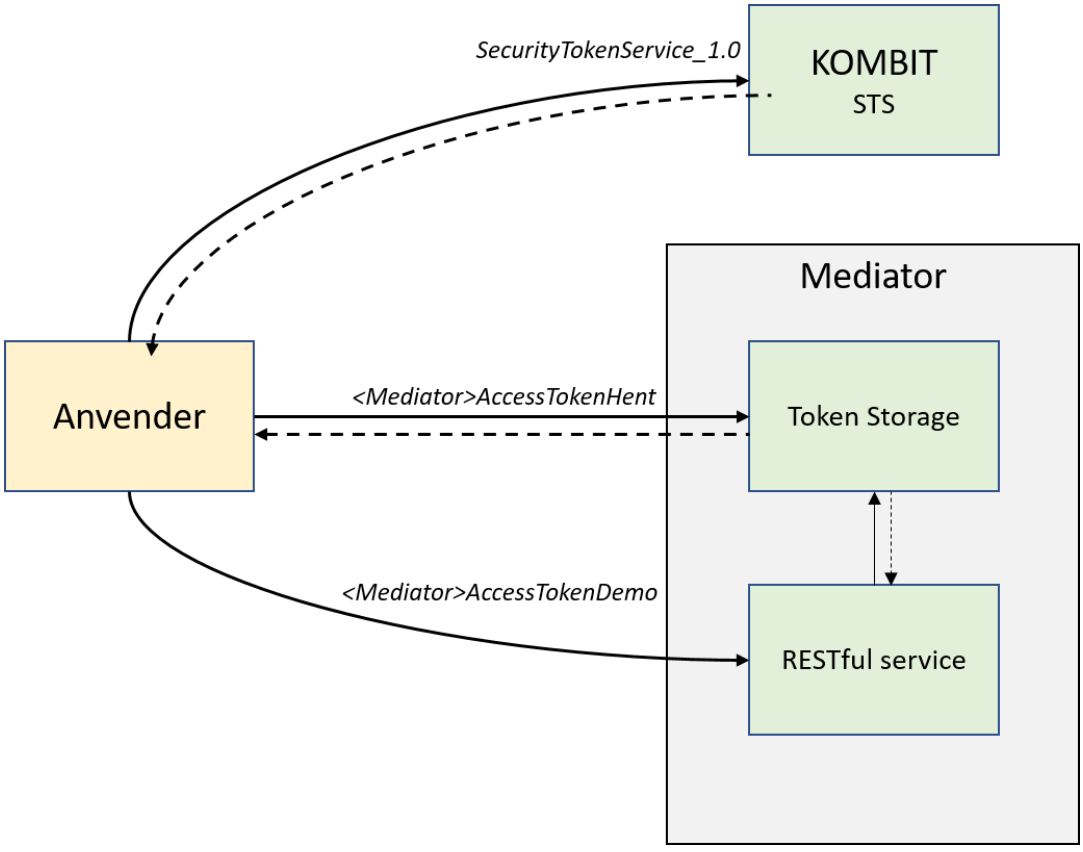
Detaljerne i løsningen er beskrevet i [REST Sikkerhed].

Integrationen stiller desuden en demo RESTful webservice, <*Mediator*>AccessTokenDemo, til rådighed, så man kan teste, at man kan hente og anvende Access token korrekt. <*Mediator*>AccessTokenDemo vil modtage det Access Token man har modtaget fra <*Mediator*>AccessTokenHent, og slå det op i Access Token Store og validere at det oprindelige SAML-Token er gyldigt og giver den korrekte adgang. På serviceplatformen vil denne service hedde ServiceplatformAccessTokenDemo.

Oversigt over integrationens services:

Servicenavn	Beskrivelse af formål	Serviceversion
ServiceplatformAccessTokenHent	At veksle et SAML Token til et Access Token til kald af RESTful webservices på Serviceplatformen.	1.0
ServiceplatformAccessTokenDemo	Servicen gør det muligt at teste Access Token, hentet med ServiceplatformAccessTokenHent service.	1.0

Figur 1 nedenfor viser et positivt forretningsforløb for kald



1. Anvendersystem kalder SecurityTokenServiceUdgående (se SF1514 https://docs.kombit.dk/integration/sf1514) og får udstedt et SAML token
2. Anvendersystem kalder ServiceplatformAccessTokenHent med SAML Token, og får returneret et Access Token
3. Anvendersystem kalder ServiceplatformAccessTokenDemo med Access Token i headeren, og får en status for kaldet tilbage

3. VILKÅR OG BETINGELSER

Der er ingen særlige vilkår for brug af nærværende integration ud over de Generelle vilkår, der er beskrevet under vilkår for hhv. leverandører og kommuner i Digitaliseringskataloget

3.1. Service Level Agreement (SLA) og åbningstider

Information om SLA og åbningstider for den fælleskommunale infrastruktur findes i Digitaliseringskataloget.

4. TEST

4.1. Testfaciliteter og testmiljø

Korrekt brug af ServiceplatformAccessTokenHent kan verificeres ved kald af ServiceplatformAccessTokenDemo, i både test- og produktionsmiljø.

Der stilles en testklient til rådighed, som gør det muligt at test services. Detaljer herom kan findes i servicebeskrivelserne.

4.2. Testdata

Der eksisterer ikke særskilte testdata for disse services.

4.3. Test i forbindelse med produktionssætning

Brug af ServiceplatformAccessTokenHent er en forudsætning for kald af andre RESTful webservices, og testes derfor som en del af integrationstest af disse services.

5. OPGAVER IFM. IBRUGTAGNING AF INTEGRATIONEN

Anvendelsen af SF1516 bygger på en forudgående anvendelse af Security Token Service (SF1514), og derfor gælder samme forudsætninger for tilslutning som for SF1514. Derudover er der ikke yderligere forudsætninger.

6. LOVHJEMMEL

Du kan læse om vilkårene for brug af den fælleskommunale infrastruktur i Digitaliseringskataloget – herunder om kravene til lovlig adgang til data.

6.1. Lovhjemmel for KOMBIT-anvendersystemer

Hvis denne integration benyttes af et eller flere KOMBIT-anvendersystem(er), fremgår lovhjemmel for deres brug af denne oversigt.

Det anførte hjemmelsgrundlag er bestemt af det enkelte fagprojekt på bestillingstidspunktet på baggrund af en rimelig og dækkende analyse. Henvisningen til hjemmelsgrundlaget bliver derfor ikke nødvendigvis vedligeholdt, hvorfor KOMBIT naturligvis ikke kan indestå for, at retsvirkning til alle tider vil være korrekt.

Bemærk, at denne integrations services blot understøtter brug af andre services, og derfor ikke giver særskilt adgang til data, udover hvad de understøttede services giver adgang til. Hjemmelsgrundlaget vil derfor skulle holdes op imod adgangen til data i de understøttede services.

REFERENCER

Ref	Titel	Beskrivelse
[OIOIDWS]	OIO IDWS REST Profile V1.0, Digitaliseringsstyrelsen	Digitaliseringsstyrelsens profilering af OIOIDWS standarden. https://docs.kombit.dk/weblokation/202103250949
[REST Sikkerhed]	Kombit REST Sikkerhedskrav.pdf	Specifikation af implementeringen af OIOIDWS for KOMBITs RESTful webservices [https://docs.kombit.dk/integration/sf1516/1.0/pakke]/ Kombit REST Sikkerhedskrav.pdf