



SF1518 Sikkerhed - Administrationsmodul webservice enabling

Integrationsversion 2.1.0

Integrationsbeskrivelse

Kommunernes Data & Infrastruktur - KDI

Versionshistorik

Integrations version	Dokument version	Initialer	Dato	Kommentarer
	0.1	XKHI	2020-04-02	Første version
2.1.0		XKHI	2020-04-21	Opdateret til Digitaliseringskataloget

Referencer

Ref.	Titel	Kommentarer
[SikkerhedVejledning]	"Vejledning til Adgangsstyring for brugere (til leverandører) v.0.2.pdf"	Digitaliseringskatalogets informationsside om den samlede adgangsstyringsløsning i den fælleskommunale rammearkitektur kan findes her: http://docs.kombit.dk/loesning/adgangsstyring/betingelse
[STS-VILKÅR]	"Bilag 2 - Vilkår for anvendelse af sikkerhedsmodellen i Rammearkitekturen version 2.2"	Digitaliseringskatalogets informationsside om den samlede adgangsstyringsløsning i den fælleskommunale rammearkitektur kan findes her: http://docs.kombit.dk/loesning/adgangsstyring/betingelse

Indholdsfortegnelse

1	Overordnet beskrivelse	4
1.1	Integrationens formål	4
1.2	Forudsætninger for produktionssætning	4
1.2.1	Særlige vilkår	4
1.2.2	Supplerende information om tilslutning	4
2	Kontekst for integrationsparter	5
2.1	Kontekst for Brugervendt system	5
2.1.1	Lovhjemmel og forvaltningsmæssigt formål	5
2.1.2	Ønsker og forventninger til kapacitets- og servicekrav fra denne integrationspart.....	5
2.1.3	Specifikke forudsætninger for tilslutning af denne integrationspart.....	5

1 Overordnet beskrivelse

1.1 Integrationens formål

Formålet med integrationen er at kunne opdatere IT-systemer og Jobfunktionsroller via et Api.

It-leverandører kan opdatere eksisterende serviceudbydere og brugervendte systemer og myndigheder kan oprette, opdatere og slette jobfunktionsroller.

Nærværende dokument giver et overordnet indblik i, hvilke aktiviteter man som anvender, skal igennem for at bruge Api'et. Detailgennemgang og vejledning i aktiviteter man skal gennemgå, kan læses i vejledningen, som findes i referencen [Sikkerhedsvejledning]. Specifikt henvises til **Dokumentation til Administrationsmodulets API og Vejledning til Administrationsmodulets API**.

Bemærk i øvrigt vilkår for anvendelse af integrationen, der kan læses i [STS-VILKÅR].

1.2 Forudsætninger for produktionssætning

For at benytte integrationen er det nødvendigt, at der i Administrationsmodulet er tilknyttet et klientcertifikat af typen VOCES eller FOCES på den organisation (myndighed eller it-leverandør) som skal benytte integrationen.

1.2.1 Særlige vilkår

Se [STS-VILKÅR].

1.2.2 Supplerende information om tilslutning

Intet.

2 Kontekst for integrationsparter

2.1 Kontekst for Brugervendt system

2.1.1 Lovhjemmel og forvaltningsmæssigt formål

Ikke relevant.

2.1.2 Ønsker og forventninger til kapacitets- og servicekrav fra denne integrationspart

Ikke relevant.

2.1.3 Specifikke forudsætninger for tilslutning af denne integrationspart

Dette kapitel beskriver de opgaver, som skal gennemføres i relation til snitfladen.

ID	Aktivitet	Opgave-kategori	Komponent	Ansvarlig	Udførende	Fase og afhængighed	Kommentar
TS101	Foretag risiko-vurdering	Sikkerhed	System	Leverandør	Leverandør	Fase 1	
TS102	Bestilling af FO-CES-certifikat til system.	Koordination	Nets	Leverandør	Leverandør	Fase 2	
TS103	Indlæs certifikat i Administrationsmodulet under den Organisation hvis kontekst API'et skal anvendes.	Koordination	Administrationsmodul	Leverandør	Leverandør	Fase 2	
TS104	Systemet er klar til at kunne anvende API'et.	Koordination	Administrationsmodulets Api	Leverandør	Leverandør	Fase 2	

TS101	-	Det er et krav for tilslutning til KOMBITs rammearkitektur, at der foretages en risikovurdering med henblik på at afdække konsekvenser ved anvendelse af Api'et.
-------	---	--

TS102	-	Som led i tilslutningen af et system til Api'et skal leverandøren bestille et FO-CES-certifikat, som skal anvendes af systemet til autentifikation.
TS103	-	Certifikatet skal være oprettet i ADM under egen organisation. Bemærk, en organisation må gerne have flere certifikater tilknyttet (dog maks. 2), f.eks. kunne der være flere systemer der må tilgå Administrationsmodulets eksterne snitflade på vegne af denne organisation. Tilføj certifikatet ved at trække det ind på det markerede område. Filen kan f.eks. genereres ved at eksportere certifikatet i Windows certmgr, anvend format "Base-64 encoded X.509 (.CER)". Filtypen skal være .cer eller .crt. Certifikatet skal være unikt og må ikke genanvendes for andre organisationer. Certifikatet skal være et VOCES- eller FOCES-certifikat og det skal være i PEM-format. Certifikatet må ikke være udløbet.