KOMBIT

Kommunernes it-fællesskab

SF1511 Sikkerhed - Hent token fra Context Handler

Integrationsversion 2.1

Integrationsbeskrivelse

Kommunernes Data & Infrastruktur - KDI

Versionshistorik

Integrations version	Dokument version	Initialer	Dato	Kommentarer
	0.1	ehe	2015-07-01	Første version
	2.1.0	ehe	2015-07-01	Indarbejdet reference til STS
	2.1.1	JJN	2016-09-02	Opdateret med forudsætninger og vilkår for tilslutning er tilføjet. - Kapitel 1.1 - Generelt - Kapitel 2.1 - Aktiviteter
	2.1.2	JJN	2016-12-12	Opdatering af kapitel 2.1 -TS104: Certifikat er knyttet til IdP og ikke Brugervendt system.
	2.1.3	XEHL	2018-07-03	Opdateret links i Referencer, da dokumenter er f lyttet. Opdateret reference [Sikkerhedsvejledning], med opdateret vejledningsdokument. Mindre redaktionelle rettelser.
2.1.3		RHI	2020-02-03	Opdateret til Digitaliseringskataloget
2.1.3		RHI	2020-04-02	Fjernelse af gamle links til share-komm og tilføjelse af afsnit 1.1.4 med links til Context Handler for hhv produktion og testmiljø
2.1		RHI	2021-06-10	Tilpasset KOMBIT dokument versionering strategi Opdateret TS101 Fjernet TS102 Anmeld Anvendesystem til datatilsynet, da det refererede til krav fra den gamle persondatalov.

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
[OIOSAML]	OIOSAML hos Digitaliseringsstyrelsen	https://digitaliser.dk/group/42063/resources

Indholdsfortegnelse

1 Overordnet beskrivelse

Nærværende dokument beskriver hvordan et fagsystem integrerer med Context Handler. Dette gøres ved at etablere en SAML integration mellem fagsystemet og CContext Handler, samt en SAML integration mellem CContext Handler og myndighedernes Identity Provider (IdP). Fagsystemet kan derved sende brugere med et login-request til Context Handler, som sender login-request videre til myndighedens lokale IdP. Den lokale IdP beriger SAML Token med brugers jobfunktionsroller og Context Handler oversætter disse til brugersystemroller, inden brugeren til sidst sendes tilbage til fagsystemet. Hele processen foregår ved client redirects. Føderationerne konfigureres ved hjælp af certifikater og SAML metadata. Dette er beskrevet i detaljer i [SikkerhedVejledning]. Det forudsættes at læser er bekendt med SAML og OIOSAML.

Denne integrationsbeskrivelse giver et overordnet indblik i hvilke aktiviteter man som anvender skal igennem for at bruge Adgangsstyring for brugere. Detailgennemgang og vejledning i aktiviteter man skal gennemgå, kan læses i vejledningen, som findes i referencen [Sikkerhedsvejledning]. Specifikt henvises til Appendiks A og SAML beskederne **AuthnRequest** samt **SAMLResponse**.

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

1.1 Forudsætninger for produktionssætning

Tilslutning til Context Handler sker ved at tilslutning KOMBITs rammearkitektur, i praksis når Brugervendt system oprettes i administrationsmodulet.

1.1.1 Køreplan for Implementering

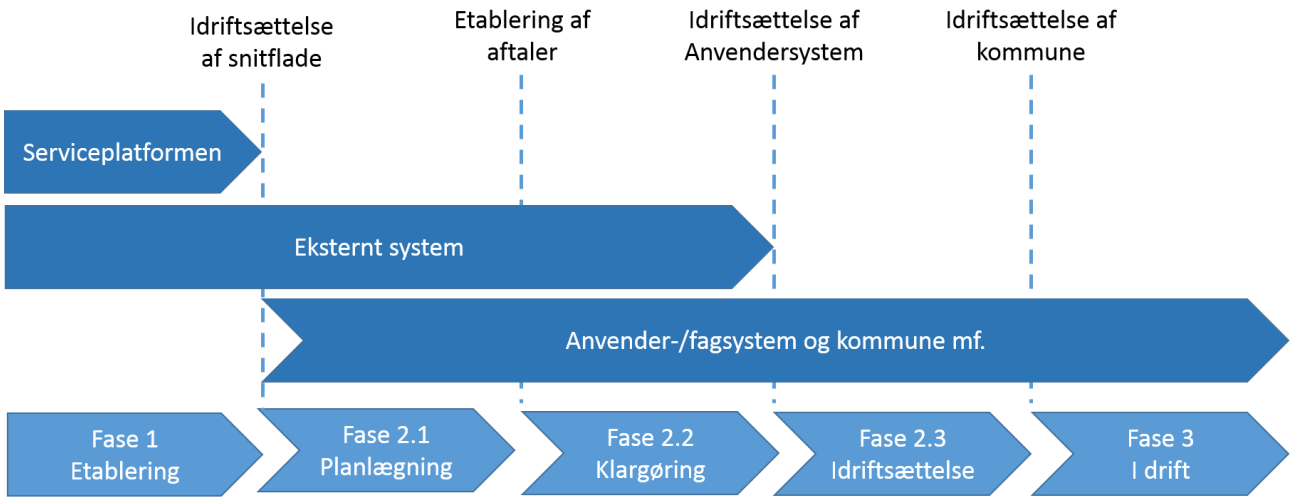
Nedenstående diagram viser køreplanen for udrulningen af et Brugervendt system inden for KOMBIT rammearkitektur under monopolbrudsprojektet. Det væsentlige i køreplanen er faserne, mens en egentlig tidsplan vil følge af den faktiske implementeringsplan. Aktiviteter, som er forudsætninger og betingelser i forbindelse med ibrugtagning af en snitflade, som følge af en udrulning af et Brugervendt system, vil referere til den fase, den hensigtsmæssig kan udføres i.

Context Handler er ikke vist i diagrammet nedenfor, men ved idriftsættelse, er services beskrevet i denne snitflade klar til anvendelse. Idriftsættelse af Context Handler er en fase 1 aktivitet.

Serviceplatformen: Ved idriftsættelse af en snitflade er alle aktiviteter afsluttet, og snitfladen er klar til anvendelse.

Kildesystem: Alle aktiviteter i forhold til serviceplatformen er afsluttet, men der kan være yderligere aktiviteter i forbindelse med tilslutning af et Brugervendt system eller en kommune i forhold til kildesystemet.

Brugervendt system og kommune: Ved tilslutning af et Brugervendt system og/eller en kommune, er der en række aktiviteter op til idriftsættelse, dels af aftalemæssig karakter, og dels også af konfigurationsmæssig karakter, som skal udføres. Er der aktiviteter, som medfører konfiguration på Serviceplatformen, vil dette ske i forbindelse med leverandørens oprettelse af serviceaftalen for kommunen.



1.1.2 Særlige vilkår

Se [STS-VILKÅR].

1.1.3 Supplerende information om tilslutning

Intet.

1.1.4 Link til Context Handler

Ekstern Test

For Brugervendt System

https://adgangsstyring.eksterntest-stoettesystemerne.dk/runtime/saml2/metadata.idp

For Kommunal IdP

https://adgangsstyring.eksterntest-stoettesystemerne.dk/runtime/saml2auth/metadata.idp

Produktion

For Brugervendt System

https://adgangsstyring.stoettesystemerne.dk/runtime/saml2/metadata.idp

For Kommunal IdP

https://adgangsstyring.stoettesystemerne.dk/runtime/saml2auth/metadata.idp

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

Brugervendt system bør orientere KOMBIT om forventet kapacitetsbehov for denne integration.

2.1.3 Specifikke forsætninger for tilslutning af denne integrationspart

Dette kapitel beskriver de opgaver, som skal gennemføres i relation til snitfalden, for at en kommune gennem et Brugervendt system kan benytte snitfladen.

ID	Aktivitet	Opgave-kategori	Kompo-nent	Ansvarlig	Udførende	Fase og afhæn-gighed	Kommentar
TS101	Opdater GDPR Dokumentation	Sikkerhed	Bruger-vendt sy-stem	Fagprojekt	Leverandør af Bruger-vendt sy-stem	Fase 1	Benytter Brugervendt systemet også SF1512 1514 kan dette punkt dækkes i samme do-kumentation
TS102	Udgået						
TS103	Verificer at den Kommunale IdP har FOCES cer-tifikat til føde-ra-tionsaftale med Contexthandler	Verifika-tion	STS Con-text Handler	Kommune	Kommune	Fase 1	
TS104	Anmod om af-tale om føde-ration mellem myndigheds IdP og Context Handler	Aftale	STS Con-text Handler	Kommune	Kommune	Fase 1	
TS105	Oprettelse af fø-derationsaftale i Contexthandler mellem IdP og Context Handler	Konfigura-tion	Admini-strations-modul	KDI	KDI	Fase 2.2	

TS106	Bestilling af FOCES certifikat til Brugervendt system.	Koordination	Nets	Leverandør af Brugervendt system	Leverandør af Brugervendt system	Fase 2.2	Certifikatet benyttes genereret af Brugervendt systemet og kommune ved tilslutning.
TS107	Fastlæggelse af Brugersystemroller	Koordination	Administrationsportal	Leverandør af Brugervendt system	Leverandør af Brugervendt system	Fase 2.2	
TS108	Fastlæggelse af Jobfunktionsroller for Brugervendt system og mapping til Brugersystemroller	Koordination	Administrationsportal	Kommune	Kommune	Fase 2.2	
TS109	Konfigurer af Brugersystemroller og Jobfunktionsroller for Brugervendt system	Konfiguration	Administrationsportal	Leverandør af Brugervendt system	Leverandør af Brugervendt system	Fase 2.2	
	Konfiguration af føderation mellem Brugervendt system og Context Handler	Konfiguration	Administrationsportal	Leverandør af Brugervendt system	Leverandør af Brugervendt system	Fase 2.2	
	Implementering af Jobfunktionsroller i lokale IdP	Konfiguration	Kommune IdP			Fase 2.2	

TS101	-	Det er et krav for tilslutning til KOMBITs rammearkitektur, at der foretages en opdatering af eksisterende GDPR Compliance dokumentation for systemet, hvoraf risikovurderingen er et af relevante dokumenter med henblik på at afdække konsekvenser ved tab af fortrolighed, integritet eller tilgængelighed i løsningen.
TS102	-	Udgået
TS103	-	Kommune skal sikre at deres lokale Identity Provider er udstyret med et FOCES certifikat, som kan anvendes i forbindelse med føderationsaftale med Context Handler.
TS104	-	Kommunen skal indsende en føderationsaftale til KOMBIT, som inkludere en række stamdata oplysninger og kommunes FOCES certifikat for Identity provider. Følgende oplysninger skal indsendes:

		• FOCES certifikat • CVR-nr. • Kontakt e-mail • SAML metadatafil fra Kommunes Identity provider • Dato for idriftsættelse. Der findes vejledninger i forhold til dette i [SikkerhedVejledning] • Føderationsaftale anmodning På sigt vil dette ske med en metadatafil, som kommunen selv vil være i stand til at ligger ind med Administrationsmodulet, og herme kan TS105 springes over. Kommunen skal i Fælleskommunal Administration oprette et IT System med rollen ”Identity Provider” og angive SAML Metadata fra den lokale IdP.
TS105	-	Kombit KDI skal konfigurere føderationsaftale for kommunes Identity Provider i Context Handler. Kommune skal i Fælleskommunal Administration anmode om føderationsaftale med den oprettede Identity Provider
TS106	-	Som led i tilslutningen af et Brugervendt system til KOMBITs rammearkitektur skal leverandørende bestille et FOCES certifikat, som skal anvendes af Brugervendt systemet til autentifikation, kryptering, indgåelse af serviceaftaler og signering ved servicekald. Kommunen skal i Fælleskommunal Administration oprette fagsystemet som IT System med rollen ”Brugervendt system” og her angive SAML metadata fra FOCES certifikat der anvendes til etablering af Trust mellem parterne.
TS107	-	Leverandøren af Brugervendt systemet skal have defineret og beskrevet Brugervendt systemets brugersystemroller, så disse kan konfigureres i Context Handler.
TS108	-	Kommunen skal definere og danne en Jobfunktionsrollemodel i Fælleskommunal Administration. Kommunen skal mappe de Jobfunktionsroller fra kommunes Identity Provider til dem der skal anvendes i KOMBITs Context Handler. I langt de fleste tilfælde vil dette være være en 1-1 model. Kommunen og leverandøren af Brugervendt systemet skal relatere Jobfunktionsrollerne til de relevante brugersystemroller. Der findes vejledninger i forhold til dette i [SikkerhedVejledning] • Vejledning til udarbejdelse af jobfunktionsroller for kommuner

TS109	-	Brugervendt system skal være oprettet i det Fælleskommunale Administrations-modul og rollemodellen fra TS108 skal være konfigureret. Der findes vejledninger i forhold til dette i [SikkerhedVejledning] • Ibrugtagning STS - Adgangsstyring for brugere På sigt vil dette ske med en metadatafil, som leverandøren selv vil være i stand til at ligger ind med Administrationsmodulet. Ligeledes vil det på sigt være muligt at oprette og vedligeholde Jobfunktionsrolle gennem SF1518.