KOMBIT
Kommunernes it-fællesskab

NOTAT

Bilag 11: Anvenderkrav til adgangsstyring - Støttesystemerne Context handler, Security Token Service og Administrationsmodul

(Bilag til dagsordenspunkt 8, Kommunale anvenderkrav til støttesystemerne)

Referencer:

[AOVERSIGT]	Oversigt over Adgangsstyring i rammearkitekturen, Dokumentet er under udarbejdelse og ikke offentliggjort endnu. (Seneste offentligt tilgængelige materiale om Adgangsstyring er Kravspecifikation for Adgangsstyring og Kravspecifikation for Administrationsmodulet, version 1.0 marts 2013. Læseren henvises særligt til afsnit 3.1 i ” ”Kravspecifikation for Administrationsmodul for Adgangsstyring version 1.0” for en oversigt over begreber, der anvendes i dette notat.)

1. Indledning og vejledning

I forbindelse med det forestående monopolbrud konkurrenceudsætter KOMBIT indkøb af Fælleskommunale Støttesystemer, der er en del af den Fælleskommunale Rammearkitektur. Det forventes at Støttesystemerne indkøbes i løbet af 2013 og vil kunne tages i brug i 2014, men landets kommuner bør allerede inden begynde at tage højde for Støttesystemerne i kommende udbud.

Nærværende vejledning henvender sig primært til de personer i kommunerne, der beskæftiger sig med at udarbejde kravspecifikationer og andet materiale i forbindelse med it-udbud. Vejledningen giver et forslag til, hvordan krav til adgangsstyring i henhold til den fælleskommunale rammearkitektur kan indgå i kommunens kommende udbud. Kommunen bør sikre, at forslagene passer til de konkrete kontrakter, hvori brug af rammearkitekturen indgår.

Adgangsstyring i rammearkitekturen understøttes af tre støttesystemer:

- Security Token Service, der understøtter adgangsstyring når et anvender-system ønsker at tilgå et støttesystem.
- Context Handler, der understøtter adgangsstyring når en bruger ønsker adgang til et anvendersystem.
- Administrationsmodulet, der anvendes til at opsætte aftaler om hvilke systemer der må tilgå rammearkitekturen og hvad disse systemer har adgang til, samt administrere hvordan de enkelte systemer understøtter adgangskontrol.

Denne vejledning er en samlet beskrivelse af de krav, der stilles til systemer der anvender alle tre støttesystemer.

Støttesystemerne Security Token Service og Context Handler er kravspecificeret i dokumentet ”Kravspecifikation for Adgangsstyring version 1.0.docx” mens støttesystemet Administrationsmodul er kravspecificeret i dokumentet ”Kravspecifikation for Administrationsmodul for Adgangsstyring version 1.0.docx”.

OBS: Kravene i denne vejledning er baseret på ovenstående kravspecifikationer. Disse kravspecifikationer forligger endnu ikke i en endelig version. Kravene i dette dokument må derfor forventes at kunne blive ændret og udbygget i takt med at kravspecifikationerne færdiggøres!

Kravene i nærværende notat beskrives ved brug af den terminologi og de begreber, der er beskrevet i [AOVERSIGT]. Læseren antages at være bekendt med terminologi og begreber.

Læsevejledning

[Tekst med denne markering i de efterfølgende afsnit er forklarende tekst og vejledning.]

Øvrig tekst er krav og bestemmelser, der kan anvendes i forbindelse med udbud af it-systemer.

Når der i denne vejledning benyttes begrebet Systemet menes der det system, der bliver udbudt. Når der i denne vejledning benyttes begrebet Leverandøren, menes der tilbudsgivere i forbindelse med udbuddet og senere leverandør af Systemet.

Når der i denne vejledning benyttet begrebet Myndighed menes den en kommune eller anden offentlig Myndighed. Hvis en kommunen anvender krav i denne vejeledning i forbindelse med et it-udbud vil der Myndighed altså henvise til kommunen, der er kunde i it-udbuddet.

Opdeling og brug af dokumentet

Dokumentet er opdelt i en række afsnit, der afspejler de forskellige typer af systemer, der optræder i rammearkitekturen, nemlig anvendersystem, støttesystem og anvendersystem med brugeradgang. I et givet it-udbud vil det udbudte system ikke nødvendigvis skulle optræde som alle disse typer af systemer og det er derfor ikke nødvendigvis relevant at medtage alle afsnit i givet it-udbud. Kommunen bør sikre, at man nøje overvejer hvilke krav, der vil være relevante at medtage i et givet udbud. Nedenfor beskrives hvornår de forskellige afsnit vil være relevante at medtage.

Dokumentet er opdelt i følgende afsnit:

- Afsnit 2 ”Krav til Leverandørens anvendelse af rammearkitekturens administrationsmodul”
- Afsnit 3 ”Krav til adgangsstyring for anvendersystemer”
- Afsnit 4 ”Krav til adgangsstyring for støttesystemer”
- Afsnit 5 ”Krav til adgangsstyring for anvendersystemer med brugeradgang”
- Afsnit 6 ”Ikke-funktionelle krav vedrørende adgangsstyring”

Afsnit 2 og Afsnit 6 vil være relevante for alle Leverandører og systemer, der skal tilkobles rammearkitekturen.

Afsnit 3 beskriver krav til hvordan anvendersystemer skal anvende adgangsstyringen i rammearkitekturen. Disse krav er relevante for alle systemer, der ønsker at anvende services fra et af rammearkitekturens støttesystemer.

Afsnit 4 beskriver krav til hvordan støttesystemer skal håndtere adgangsstyring. Disse krav er relevante for alle systemer, der ønsker at udstille en service som et støttesystem under den fælleskommunale rammearkitektur.

Afsnit 5 beskriver krav til hvordan et anvendersystem kan foretage adgangsstyring for brugere i henhold til rammearkitekturens føderationsmodel for adgangsstyring. Disse krav kan være relevant for alle brugervendte systemer, der tilkobles rammearkitekturen. Det er dog ikke obligatorisk at adgangsstyring for brugervendte systemer foregår i henhold til rammearkitekturens adgangsstyringsmodel, for at et givet system kan optræde som et anvendersystem i rammearkitekturen. I forbindelse med et it-udbud bør kommunen nøje overveje fordele og ulemper ved at anvende rammearkitekturens model for adgangsstyrring for brugere. Vurderingen af fordele og ulemper vil i høj grad afhænge af kommunens samlede strategi for bruger- og rettighedsstyring.

[AOVERSIGT] beskriver en oversigt over adgangsstyring i rammearkitekturen. Dette vil kunne vedlægges som informationsbilag til Leverandøren i forbindelse med et udbud.

2. Krav til Leverandørens anvendelse af rammearkitekturens administrationsmodul

[For alle systemer, der skal anvende rammearkitekturen skal systemet oprettes og administreres i rammearkitekturens administrationsmodul i henhold til krav i dette afsnit. Kravene i dette afsnit bør stilles såfremt man ønsker at Leverandøren skal foretage oprettelse og administration at Systemet i rammearkitekturens administrationsmodul.]

For at Systemet kan anvende rammearkitekturen skal Leverandøren oprettes i som tilslutningspart i rammearkitekturs administrationsmodul og Leverandøren skal oprette en tilslutningsaftale for Systemet i administrationsmodulet.

2.1 Krav til oprettelse som tilslutningspart

Krav #1	**Oprettelse af tilslutningspart**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Leverandøren skal oprette sig som tilslutningspart i rammearkitekturens administrationsmodul for kunne tilslutte systemer til rammearkitekturen og redigere aftaler og roller for disse.		

Krav #2	**Tilknytning af underskriftberettiget**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Leverandøren af Systemet skal have tilknyttet en underskriftsberettiget, der er oprettet i CVR der logger op rammearkitekturens administrationsmodul med ved anvendelse af et OCES medarbejder certifikat.		

Krav #3	**Administratorer**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Leverandøren af Systemet skal udpege en eller flere administratorer i Leverandørens organisation. Disse skal kunne logge på rammearkitekturens administrationsmodul ved anvendelse af et OCES medarbejder certifikat.		

2.2 Krav til oprettelse af tilslutningsaftaler

Krav #4	Etablering af aftale om tilslutning		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Leverandøren af Systemet er ansvarlig for at anmode om tilslutning af Systemet til specifikke dele af rammearkitekturen via rammearkitekturens administrationsmodul. Leverandøren af Systemet skal anvende rammearkitekturens administrationsmoduls brugergrænseflade til dette formål.		

Krav #5	Oprettelse af tilslutning		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Leverandøren af Systemet er ansvarlige for at Systemet som en del af tilslutningen oprettes i rammearkitekturens administrationsmodul med konfigurationsoplysninger om Systemet, herunder IP-adresse, SAML metadata inkl. et OCES certifikat, der identificere systemet.		

Krav #6	Vedligehold af tilslutning		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Leverandøren af Systemets er ansvarlig for at konfigurationsoplysninger for tilslutningen er korrekte og løbende opdateres, herunder at certifikater opdateres inden udløb.		

3. Krav til adgangsstyring for anvendersystemer

[Såfremt Systemet er et anvendersystem skal Systemet opfylde de krav, der er beskrevet i dette afsnit for at kunne få adgang til støttesystem. Et anvendersystem er et system, der har behov for adgang til et af rammearkitekturens støttesystemer].

Adgang til støttesystemer kræver at der er indledningsvis er oprettet en afsendersystemaftale eller en serviceaftale for at få adgang til det enkelte støttesystem.

Såfremt Systemet har brug for at opdatere støttesystemets data skal der etableres en afsendersystemaftale, der beskriver hvilke data det må opdateres. Såfremt Systemet har brug for at modtage støttesystemets data skal der etableres en serviceaftale, der beskriver hvilke data det må modtage. Begge aftaler oprettes via i rammearkitekturens administrationsmodul.

I praksis kræver adgang til et støttesystem at anvendersystemet har en gyldig Security token, der medsendes til kald af støttesystemet. Security token'et udstedes til anvendersystemet af rammearkitekturens Security Token Service.

3.1 Krav til oprettelse og vedligehold af aftaler

[Kravene i dette afsnit er relevante såfremt Leverandøren at Systemet skal være ansvarlig for at administrere aftaler for Systemet.]

Krav #7	Etablering af afsendersystemaftaler		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Leverandøren af Systemet er ansvarlig for at anmode om nye afsendersystemaftaler, der er nødvendige for at Systemet kan ændre data et rammearkitekturens støttesystemer. Leverandøren af Systemet skal anvende rammearkitekturens administrationsmoduls brugergrænseflade til dette formål. I denne proces skal eksempelvis Systemets OCES certifikat og EntityID registreres.		

Krav #8	Etablering af serviceaftaler		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Leverandøren af Systemet er ansvarlig for at anmode om nye serviceaftaler, der er nødvendige for Systemet brug af rammearkitekturens støttesystemer. Leverandøren af Systemet skal anvende rammearkitekturens administrationsmoduls brugergrænseflade til dette formål. I denne proces skal eksempelvis Systemets OCES certifikat og EntityID registreres.		

Krav #9	Vedligehold af afsendersystemaftaler		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Leverandøren af Systemet er ansvarlig for at vedligeholde indgåede aftaler ved at foretage nødvendige ændringsanmodninger til eksisterende afsendersystemaftaler. Leverandøren af Systemet skal anvende Administrationsmodulets brugergrænseflade til dette formål.		

Krav #10	Vedligehold af serviceaftaler		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Leverandøren af Systemet er ansvarlig for at vedligeholde indgåede aftaler ved at foretage nødvendige ændringsanmodninger til eksisterende serviceaftaler til Systemets brug af rammearkitekturen Leverandøren af Systemet skal anvende rammearkitekturens administrationsmoduls brugergrænseflade til dette formål.		

3.2 Krav til integration med Security Token Service

Krav #11 er kun relevant såfremt der ikke anvendes en klient mellem Systemet og Støttesystemet]

Krav #11	Brug af Security Token Service		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Systemet skal benytte Security Token Service komponenten i rammearkitekturen til at få udstedt SAML Security Tokens forud for kald af adgangsbegrænsede services, der udstilles af støttesystemer. Security Token Service kaldes med en WS-Trust <RequestSecurityToken > besked.		

[En Myndighed har mulighed for at anvende den fælles Security Token Service, der tilbydes at rammearkitekturen. Alternativet, kan Myndigheden opstille en lokal Security Token Service.

Krav #12 er kun relevant såfremt Myndigheden anvender den fælles Security Token Service. I dette tilfælde udgår krav #13.]

Krav #12	Integration til Security Token Service		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Systemet skal integrere til Security Token Servicen i rammearkitekturen enten med OIO WS-Trust profilen af OASIS WS-Trust standarden, som Security Token Servicen tilbyder. Kald til Security Token Servicen signeres med det OCES certifikat som er tilknyttet den specifikke aftale på det data som der kaldes efter.		

Det er under overvejelse også at tilbyde et REST interface.

[Krav #13 er kun relevant såfremt Myndigheden anvender en lokal Security Token Service. I dette tilfælde udgår krav #12.]

Krav #13	Integration til lokal Security Token Service		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Systemet skal integrere til Myndighedens lokale Security Token Servicen enten med OIO WS-Trust profilen af OASIS WS-Trust standarden eller med det REST interface, som Security Token Servicen tilbyder. Kald til Security Token Servicen signeres med et certifikat, der på forhånd er udvekslet med den lokale Security Token Service.		

3.3 Krav til anvendelse af støttesystemer

Krav #14	Anvendelse af adgangsbegrænsede støttesystem services		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Systemet skal medsende gyldige security tokens hentet fra Security Token Service når adgangsbegrænsede services udstillet af støttesystemer kaldes.		

Krav #15	Cashing af security tokens		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Et SAML token må caches og anvendes så længe det er gyldigt, således at efterfølgende service-kald til samme støttesystem ikke behøver involvere forudgående kald til Security Token Servicen for at etablere et nyt security token.		

4. Krav til adgangsstyring for støttesystemer

[Krav i dette afsnit er relevante at medtage i et udbud såfremt Systemet, der udbydes, skal indgå som et støttesystem i rammearkitekturen. Et støttesystem er et system, der udstiller en service, som kan anvendes at andre systemer under den fælleskommunale rammearkitektur.]

Et støttesystem er et system, der udstiller en service, hvor adgangsbegrænsning sker i henhold til en afsendersystemaftale eller en serviceaftale, som er registeret i rammearkitekturens administrationsmodul. Der påhviler dog ikke direkte Leverandøren af støttesystemet nogen forpligtigelser i forbindelse med indgåelse af afsendersystemaftaler og serviceaftaler idet disse aftaler indgås mellem leverandøren af et anvendersystem og henholdsvis KOMBIT og de Myndigheder, hvis data udstilles.

Håndhævelsen af adgangskontrol sker ud fra en række systemroller, som defineres af støttesystemet. Disse systemroller oprettes og vedligeholdes af Leverandøren i rammearkitekturens administrationsmodul.

Støttesystemet skal efterfølgende håndhæve adgangskontrol på baggrund af security tokens, der udstedes af rammearkitekturens Security Token Service. Disse security tokens medsendes i servicekald til støttesystemet og indeholder attributter, der beskriver hvilke systemroller et anvendersystem har.

4.1 Krav til oprettelse og vedligehold af systemroller

Krav #16	**Systemroller**		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Systemet skal understøtte adgangskontrol ud fra en række systemroller. Systemroller skal være kompatible med rammearkitekturens begrebs- og informationsmodel for Adgangsstyring. Systemrollerne anvendes udadtil til modellering og administration af Systemers adgang. Alle systemroller tildeles i kontekst af en organisation (f.eks. på vegne af en kommune). Systemroller skal repræsenteres eksternt som en unik URI (med et systemspecifikt præfiks).		

Krav #17	**Oprettelse af systemroller**		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Leverandøren af Systemet er ansvarlig for indledningsvist at definere en række standard systemroller til Systemet. Leverandøren af Systemet er ansvarlig for at registrere disse systemroller i rammearkitekturens administrationsmodul.		

Krav #18	Redigering af systemroller		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Det skal være muligt at redigere afbildningen mellem systemroller og Systemets interne systemrettigheder i rammearkitekturens administrationsmodul.		

Krav #19	Beskrivelse af rettighedsmodel		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Leverandøren af Systemet bedes beskrive den rettighedsmodel for brugeradgange, som anvendes internt i Systemet – herunder hvilke funktionelle afgrænsninger, dataafgrænsninger og dataklassifikationer, som systemroller kan opbygges af. Leverandøren af Systemet bedes desuden beskrive hvorledes den interne rettighedsmodel forventes at blive afbilledet til systemroller.		

4.2 Krav til håndhævelse af adgangskontrol

[Samtlige støttesystemer der er tilsluttet rammearkitekturen skal håndhæve adgangskontrol ved alle kald til støttesystemets services].

Krav #20	Håndhævelse af adgangskontrol		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Systemet skal håndhæve adgangskontrol ved alle kald til Systemets services. Adgangskontrollen skal håndhæves ud fra de attributter, der findes i den SAML security token, der medsendes til servicekaldet. Attributterne beskriver blandt andet Systemets kontekst (CVR nummer) og tildelte systemroller. Som en del af adgangskontrollen skal Systemet validere at SAML token er gyldig, herunder at den er udstedt af Security Token Servicen. Er Tokenet ikke gyldig skal adgangs til Systemet nægtes.		

Krav #21	Adskillelse mellem Myndigheder		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Adgangskontrollen skal sikre, at der er adgangsbegrænsning mellem Myndighedernes data ved at respektere den kontekst (CVR nummer), der fremgår af den modtagne SAML Assertion.		

4.3 Krav til støttesystemers klienter

[Følgende krav er kun relevante for de støttesystemer der anvender en klient til integration mellem et anvendersystem og Støttesystemet]

Krav #22	Transparent håndtering af adgangstoken		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Klienten skal håndtere adgangsstyring ved brug af Security Token Service således at det er transparent for det kaldende system.		

Krav #23	Klienters Brug af Security Token Service		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Klienten skal benytte Security Token Service komponenten i rammearkitekturen til at få udstedt SAML Security Tokens på vejne af det kaldende anvendersystem forud for kald af adgangsbegrænsede services, der udstilles af støttesystemer. Security Token Service kaldes med en WS-Trust <RequestSecurityToken > besked.		

Krav #24	Klienters Integration til Security Token Service		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Klienten skal integrere til Security Token Servicen i rammearkitekturen enten med OIO WS-Trust profilen af OASIS WS-Trust standarden, som Security Token Servicen tilbyder. Kald til Security Token Servicen signeres med det OCES certifikat som er tilknyttet den specifikke aftale på det data som der kaldes efter.		

Det er under overvejelse også at tilbyde et REST interface.

Krav #25	Klienters Integration til lokal Security Token Service		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Klienten skal kunne integrere til Myndighedens lokale Security Token Servicen enten med OIO WS-Trust profilen af OASIS WS-Trust standarden, som Security Token Servicen tilbyder. Kald til Security Token Servicen signeres med et certifikat, der på forhånd er udvekslet med den lokale Security Token Service.		

Krav #26	Klienters Anvendelse af adgangsbegrænsede støttesystem services		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Klienten skal medsende gyldige security tokens hentet fra Security Token Service når adgangsbegrænsede services udstillet af klientens støttesystem kaldes.		

Krav #27	Klienters Cashing af security tokens		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Et SAML token bør caches og anvendes så længe det er gyldigt, således at efterfølgende service-kald til samme støttesystem ikke behøver involvere forudgående kald til Security Token Servicen for at etablere et nyt security token.		

5. Krav til adgangsstyring for anvendersystemer med brugeradgang

[Krav i dette afsnit kan være relevante at medtage i et udbud såfremt Systemet, der udbydes, skal foretage adgangsstyring for brugere.

Kravene i dette afsnit skal stilles til Systemet såfremt Systemet skal foretage adgangsstyring for brugere i henhold til rammearkitekturens føderationsmodel for adgangsstyring.

Det er dog ikke obligatorisk at adgangsstyring for brugervendte systemer forgår i henhold til rammearkitekturens adgangsstyringsmodel, for at et givet system kan optræde som et anvendersystem i rammearkitekturen. I forbindelse med et it-udbud bør

kommunen nøje overveje fordele og ulemper ved at anvende rammearkitekturens model for adgangsstyrring for brugere.]

Håndhævelsen af brugerrettigheder sker ud fra en række systemroller, som defineres af Systemet. Disse systemroller oprettes og vedligeholdes af Leverandøren i rammearkitekturens administrationsmodul.

Brugeradgang håndteres efter en føderationsmodel. For et anvendersystem betyder det at det ikke behøver at kende de enkelte brugere. Anvendersystemer skal i forbindelse med bruger-login henvise brugeren til rammearkitekturens Context Handler, der sørger for at bruger-login håndteres af brugerens egen organisation. Anvendersystemet skal efterfølgende håndhæve adgang på baggrund af security tokens, der udstedes af rammearkitekturens Context Handler.

5.1 Krav til oprettelse og vedligehold af systemroller

Krav #28	**Systemroller**		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Systemet skal understøtte adgangskontrol ud fra en række systemroller. Systemets systemroller skal være kompatible med rammearkitekturens begrebs- og informationsmodel for Adgangsstyring. Systemrollerne anvendes udadtil til modellering og administration af brugernes adgange. Alle systemroller tildeles i kontekst af en organisation (f.eks. på vegne af en kommune). Systemroller skal repræsenteres eksternt som en unik URI (med et systemspecifikt præfiks).		

Krav #29	**Oprettelse af systemroller**		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Leverandøren af Systemet er ansvarlig for at indledningsvist definere en række standard systemroller. Leverandøren af Systemet er ansvarlig for at registrere disse systemroller i rammearkitekturens administrationsmodul.		

Krav #30	Redigering af systemroller		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Det skal være muligt at redigere afbildningen mellem systemroller og Systemets interne systemrettigheder i rammearkitekturens administrationsmodul.		

Krav #31	Beskrivelse af rettighedsmodel		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Leverandøren af Systemet skal beskrive den rettighedsmodel for brugeradgange, som anvendes internt i Systemet – herunder hvilke funktionelle afgrænsninger, dataafgrænsninger og dataklassifikationer, som systemroller kan opbygges af. Leverandøren af Systemet skal desuden beskrive hvorledes den interne rettighedsmodel forventes at blive afbilledet til systemroller.		

5.2 Krav til bruger-login, bruger-logout og brugersessionsstyring

Krav #32	Brugerlog-in via ContextHandler		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Log-in af brugere til Systemets web-baserede grænseflader skal håndteres via Context Handleren (SAML Identity Provider) i rammearkitekturen ved brug af OIOSAML protokollen. Systemet skal overholde OIOSAML profilen (version 2.0.9). Udestår: KOMBIT overvejer at definere en ny SAML profil baseret på OIOSAML, men med et andet sæt af attributter. Det vil så blive et krav at denne nye SAML profil understøttes. En ny SAML profil vil i givet fald blive udarbejdet i forbindelse med etablering af Context Handleren.		

Krav #33	Krav til OIOSAML Implementering		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Systemet skal i sin SAML implementering håndtere SAML AuthnRequest og SingleLogout protokollerne. Systemet skal både kunne være initierende og ikke-initierende i forhold til SAML SingleLogout.		

Krav #34	Sessionsoprettelse		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Efter log-in af brugeren udtrækkes informationer fra SAML token (modtaget fra ContextHandler) indeholdende bl.a. de systemroller, der er tildelt den aktuelle bruger for Systemet. På baggrund af indholdet af det modtagne SAML token oprettes en lokal session med brugeren, og der kan evt. ”just-in-time” oprettes en lokal brugerkonto, hvis Systemet har behov herfor. Der sker således ingen oprettelser af brugere (provisionering) forud for log-in.		

Krav #35	Sessionsstyring		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Systemet skal selv håndtere sessionsstyring med brugerens browser og herunder implementere timeout af brugersessioner ved inaktivitet i en vis periode. Det skal være muligt at konfigurere alle timeout perioder.		

Krav #36	Logout		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Systemet skal på brugergrænseflader implementere en visuel komponent til ”Logout” (via en knap eller et link), som giver brugeren mulighed for at logge af Systemet samt øvrige systemer, der har en session med ContextHandleren. Endvidere skal Systemet udstille en SOAP baseret logout mekanisme (SAML endpoint) som kan kaldes fra ContextHandleren for tvungen logout af en bruger.		

5.3 Krav til håndhævelse af adgangskontrol

Krav #37	Håndhævelse af adgangskontrol		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Systemet skal håndhæve adgangskontrol over for brugere til data og ressourcer, som Systemet har adgang til. Adgangskontrollen skal håndhæves ud fra de attributter der findes i den SAML token, der anvendes ved oprettelse af brugerens session. Attributterene indeholder blandt andet oplysninger om brugerens kontekst (CVR nummer) og tildelte systemroller. Som en del af adgangskontrollen skal Systemet validere at SAML tokenen er gyldig, herunder at den er udstedt af Context Handleren. Er Tokenet ikke gyldig skal adgangs til Systemet nægtes.		

Krav #38	Adskillelse mellem Myndigheder		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Adgangskontrollen skal sikre, at der er adgangsbegrænsning mellem Myndighedernes data ved at respektere den kontekst (CVR nummer), der fremgår af den modtagne SAML token.		

Krav #39	Delegering		
Kategori:	(K)	Type:	Funktionelt
Beskrivelse:	Systemet skal understøtte rammearkitekturens model for delegering af roller fra én organisation til en anden. Dette betyder, at modtagne SAML tokens kan indikere, at brugeren har modtaget en systemrolle på vegne af en anden organisation, end personen kommer fra. Mere specifikt vil systemrollen have en scope attribut, som indikerer et andet CVR nummer. I dette tilfælde skal Systemet give brugeren den adgang, som defineres i systemrollen, på vegne af den delegerende organisation.		

6. Ikke-funktionelle krav

6.1 Sikring af systemer, der foretager adgangsstyring

[Rammearkitekturens adgangsstyringsmodel er baseret på anvendelse af OIO SAML og OCES certifikater. Anvendersystemer og støttesystemer, der optræder som SAML end-point, skal overholde følgende krav til sikring.]

Krav #40	**Validering af tokens og certifikater.**		
Kategori:	(K)	Type:	Ikke-funktionelt
Beskrivelse:	Signaturer, certifikater og security tokens skal sikkerhedsvalideres af Systemet før brug. Der må kun accepteres SAML tokens, som er digitalt underskrevet med ContextHandlerens eller Security Token Servicens certifikat. Certifikater skal generelt spærretjekkes mod DanID.		

Krav #41	**AssuranceLevel**		
Kategori:	(K)	Type:	Ikke-unktionelt
Beskrivelse:	Leverandøren af Systemet skal definere hvilket niveau af autenticitetssikring (*level of assurance*) der er behov for for at tilgå Systemet. Leverandøren af Systemet skal anvende den fællesoffentlige referenceramme for definition af autentitetssikring[1]. Ved modtagelse af et security token skal Systemet validere, at tokenet er udstedt på mindst samme niveau, som kræves. Eksempelvis må et token med Assurancelevel=2 ikke anvendes til at tilgå et system, der kræver niveau 3. Hvis Systemet giver adgang til fortrolige eller følsomme personoplysninger, bør det krævede niveau sættes til mindst 3.		

Krav #42	**Beskyttelse af private nøgler**		
Kategori:	(K)	Type:	Ikke-Funktionelt
Beskrivelse:	Leverandøren af Systemet er ansvarlig for at beskytte private nøgler mod uautoriseret adgang – herunder de private nøgler til de OCES funktionscertifikater, som anvendes mod Context Handler og Security Token Service.		

[11] Se http://digitaliser.dk/resource/363424 for yderligere information.

Krav #43	Beskyttelse af "trust-stores"		
Kategori:	(K)	Type:	Ikke-Funktionelt
Beskrivelse:	Systemet skal beskytte de lokale trust stores (f.eks. lokale kopier af metadata og certifikater fra ContextHandler og SecuritTokenService) mod uautoriseret adgang. Det er Leverandøren af Systemets ansvar at trust stores beskyttes tilstrækkeligt.		

6.2 Andre ikke funktionelle krav

[Kommunen bør naturligvis stille andre ikke-funktionelle krav til Systemet. Herunder bør der stilles krav til logning, sikkerhed, revision, sessionsstyring, perfomance, mv. Disse krav er dog ikke specifikt møntet på adgangsstyring og er derfor ikke medtaget i dette dokument.]