Noter

20200311 SKAT Ligning sikkerhed

**Tilstede:**

Thomas Dahl Pedersen (UFST, Sikkerhedsarkitekt)  
Matthias Lund-Andersen (UFST, Løsningsarkitekt)  
Steffen W. Lang (Capgemini, Løsningsarkitekt)

**Agenda**

* Autentificering
* Sikkerhed mellem microservices i et containerbaseret setup
* Webservice sikkerhed

**Note**

Tidligere i projektet har der været tale om, at benytte AD, da SKAT Ligning ikke umiddelbart har brug for at delegere rettigheder og da SKAT Ligning frontend muligvis skulle udvikles som en dekstop applikation. På nuværende tidspunkt peger det i retning af at SKAT Ligning skal udvikles som en web applikation og DCS er derfor alligevel er relevant. Om SKAT Ligning skal udvikles som en web applikation eller en desktopapplikation afhænger af igangværende teknisk PoC. På møde afholdt med Ivan Fisher afholdt den 5. marts 2020 blev det meldt ud, at DCS er at foretrække, som sikkerhedsmodel fremfor AD, i tilfælde af det er en webapplikation der skal udvikles. Det hænger sammen med at AD-sikkerhed kræver et meget stort antal porte der skal åbnes i netværket, hvor DCS’en ikke kræver som mange portåbninger. På den baggrund blev fremtidig sikkerhedsløsning drøftet med udgangspunkt i at løsningens frontend er en web applikation og DCS benyttes som underliggende sikkerhedsmodel.

DCS er ved at blive udvidet til at understøtte SAML2. Det forventes at blive implementeret i indeværende uge. Der skal udvikles en autentificerings microservice der kan veksle en SAML2 assertion til en Json Web Token (JWT). Årsagen til dette er, at JWT er bedre velegnet ifht. Single Page Applikationer (SPA).

Nedenstående sikkerhedmodel blev skitseret på mødet og viser hvordan autentificering af bruger skal ske, hvordan sikkerhed mellem microservices implementeres og hvordan kald til SOAP webservice, udstillet af fagsystem, skal foretages. ES er valgt som et eksempel på et fagsystem der skal integreres til.



Eksempel på flow:

1. Bruger tilgår løsning via en browser og får returneret en SPA applikation (html, css, js…)
2. Bruger angiver brugernavn/password. Browser redirecter til en Authentificerings microservice.
3. Autentificerings microservice kalder DCS, som autentificerer brugernavn/password og returnerer en SAML2 assertion. Autentificerings microservice pakker SAML2 assertion ind i en Json Web Token (JWT) og returnerer den tilbage til SPA applikationen.
4. SPA-applikationen kalder Microservice #1, med JWT token, for at oprette en sag.
5. Microservice #1 kalder videre til Microservice #2, med JWT token, for at hente nogle virksomhedsoplysninger.
6. Microservice #2 udpakker JWT og kalder videre til ES med SAML2. ES tjekker rettigheder i medsendte SAML2 og returnerer virksomhedsoplysninger tilbage til Microservice #2, som returnerer virksomhedsoplysningerne tilbage til Microservice #1.
7. Microservice #1 opretter sag i database.

OMS er i gang med at udvikle en autentificerings microservice til deres brug. Det skal afklares om denne microservice kan ophøjes til en standardkomponent i UFST, og om SKAT Ligning kan genbruge denne. Thomas prøver at afklare dette.

/Steffen Lang, 11/03/20