Haderslev Kommune

TØNDER KOMMUNE

Aabenraa Kommune

Sønderborg

Sønderjysk IT-samarbejde & Single Sign On

Marts 2025

Indhold

Indledning

I kommunerne anvendes Single Sign On (herefter SSO) som adgangsstyring til IT-systemer.

Til SSO anvendes i dag KOMBITs fælleskommunale adgangsstyring (herefter benævnt FKA).

Sekundært kan anvendes Azure Single Sign On eller Active Directory Federation Services (herefter benævnt som ADFS).

Vi foretrækker i kommunerne, at SSO altid implementeres via FKA, men i nogle tilfælde accepteres SSO også via de andre muligheder. Det er af afgørende betydning, at FKA-brugerstyringen implementeres korrekt og fuldt ud. Det er altså ikke tilstrækkeligt, hvis der implementeres FKA-brugerstyring, hvor der kun anvendes enkelt-komponenter fra infrastrukturen, for eksempel en simpel validering via kommunernes identity provider. Se endvidere den nedenstående, forklarende tekst.

Dokumentet skal ses og læses som et bilag, til vores IT-tekniske udbudsmateriale, og vil bidrage med en lidt dybere teknisk beskrivelse af selve integrationen til SSO i kommunerne.

KOMBIT understøtter leverandøren med ibrugtagning af den fælleskommunale infrastruktur, herunder anvendelse af SSO: Fælleskommunal Infrastruktur

KOMBITs fælleskommunale infrastruktur

Den fælleskommunale infrastruktur understøtter central bruger- og rettighedsstyring, også kendt som single sign-on, ved hjælp af KOMBIT's fælleskommunale løsninger (tidligere Støttesystemerne/STS). Disse støttesystemer it-understøtter den mest forretningskritiske del af den kommunale sektors virksomhed og er implementerede på en række forskellige områder, herunder eksempelvis systemunderstøttelsen af et komplekst fagområde som ydelsesområdet (kontanthjælp mv.). Der er særligt to af disse støttesystemer, der er væsentlige for bruger- og rettighedsstyringens vedkommende.

Fælleskommunalt Organisationssystem (tidligere: Støttesystemet Organisation) rummer kommunens autoritative organisationsdata. Disse organisationsdata anvendes til identifikation, sagsfordeling og data-afgrænsning, for eksempel på baggrund af opmærkning med KLE-numre. Kommunerne har sin autoritative organisation indlæst på detailniveau i Fælleskommunal Organisationssystem (tidligere STS Organisation), men KLE-opmærkningen er ikke fuldstændig.

Fælleskommunal Adgangsstyring (tidligere: Støttesystemet Adgangsstyring) rummer dels forud-sætningerne for en såkaldt identity provider, dels en såkaldt security token service til autentifikation og autorisering af systembrugere.

Digitaliseringskataloget rummer mere information om disse systemer:

https://digitaliseringskataloget.dk/integrationer?f%5B0%5D=data_area%3A21&f%5B1%5D=integration_type%3AFunktionalitet

https://digitaliseringskataloget.dk/integrationer?f%5B0%5D=data_area%3A19&f%5B1%5D=integration_type%3AFunktionalitet

I kommunerne udføres den centrale bruger- og rettighedsstyring af kommunens it-service, og procedurerne fastlægges i samråd med digitaliseringsafdelingen og forvaltningsområderne.

Den fælleskommunale infrastrukturs løsninger er ikke leverandør- eller systemspecifikke, det vil sige, at denne form for bruger- og rettighedsstyring er åben for enhver leverandør, der ønsker at understøtte den. Den er allerede en integreret del af it- og systemunderstøttelsen af den kommunale sektor og vil kun blive anvendt mere.

Som al anden bruger- og rettighedsstyring hviler denne på en godkendelse (autentifikation) af en bruger, identifikation af dennes brugerrettigheder og dermed adgang til et givent system. Forløbet kan illustreres som nedenfor, de understregede begreber forklares efterfølgende:

Bruger X ønsker adgang til system Y

Bruger X valideres i brugerfortegnelsen og har brugerrettighederne Z til system Y

Bruger X logges ind i system Y med brugerrettighederne Z

Adgangen sker gennem ADFS

Valideringen sker ved, at ADFS foretager opslag i AD (brugerfortegnelsen) og udsteder en såkaldt token, der indeholder brugerrettighederne (også kendt som jobfunktionsrollen) og organisatoriske oplysninger om brugeren, der for eksempel kan tjene til dataafgrænsning.

Brugerrettighederne (jobfunktionsrollen) er enten sammensat af leverandøren eller også stiller leverandøren en slags byggesten, såkaldte brugersystemroller, til rådighed, der kan dannes en jobfunktionsrolle ud fra.

Den udstedte token giver herefter brugeren adgang til systemet.

Forudsætningen for, at de nævnte jobfunktionsroller eller brugersystemroller kan tilflyde kommunen, er, at leverandøren har registreret sin løsning på den fælleskommunale serviceplatform og udarbejdet den korrekte serviceaftale. Den pågældende serviceaftale skal herefter rettes til kommunen, som så godkender den.

Serviceplatformens hjemmeside rummer mere information om denne proces:
https://exttestwww.serviceplatformen.dk/administration/help/provider-step-by-step

Som nævnt er det af afgørende betydning, at ovenstående løsning implementeres fuldt ud. Løsninger må ikke skille eksempelvis valideringen fra tildelingen af brugerrettigheder (jobfunktionsrollen), således at sidstnævnte foretages eksempelvis i løsningens eget administrationsmodul.

Active Directory Federation Services

SAML

SAML specificerer en række kommunikationsprotokoller (kaldet Bindings), samt et beskedformat til at udveksle informationer og forespørgsler, der er relateret til autentifikation og autorisation af brugere.

Selve SAML integrationen etableres ved, at der udveksles informationer mellem it-løsningen og kommunernes ADFS, så disse kender hinanden på forhånd. Disse informationer udveksles i et SAML format, kaldet SAML Metadata (en XML struktur der indeholder oplysninger om URL end points og certifikater).

Når et it-system implementerer SAML, anvendes typisk et kode-framework der understøtter SAML protokollerne, og kan genere de beskedformater, som sendes over protokollen. Hvis man ikke har valgt framework endnu, kan det være relevant at kigge på de frameworks (OIOSAML), som Digitaliseringsstyrelsen stiller til rådighed på digitaliser.dk til hhv. Java og .NET platformen.

Rettighedsstyring

Kommunernes ADFS Miljø er bygget på et Microsoft Setup som muliggør fødereret identitet og adgangsstyring via anvendelse af vores brugerkatalog (Active Directory).

De adgangsgivende rettigheder til it-systemet bliver overført i forbindelse med brugerens login. Det sker via Claims i det SAML token, der udveksles i forbindelse med login på løsningen.

(SAML = Security Assertion Markup Language)

Rettighedstyring med SAML Claims

Brugernes rettigheder udveksles her via aftalte Claims, som defineres i forbindelse med opsætning af føderationen.

Den typiske model for håndtering af rettigheder er her, at leverandøren specificerer en række adgangsgivende roller/grupper, som kommunerne så afspejler i kommunernes AD via en Rettighedsgivende gruppe, f.eks. som eksemplificeret her

Rolle	**AD Gruppe navn**	**beskrivelse**
Administrator	<Systemnavn_>Administrator	Giver Administrativ/Fuld Adgang
Bruger	<Systemnavn_>Brugere	Giver Basis system adgang
Sagsområde1	<Systemnavn_>sagsområde1	Giver adgang til sagområde1

Eksempel på et autorisationsforløb

BrugerX skal have brugeradgang til it-systemet (ITSystemY) og arbejde med sager inden for

”Sagsområde1”.

Kommunerne sørger her for, at bruger er medlem af AD Grupperne:

”ITSystemY_Brugere” samt ”ITSystemY_sagsområde1”

Når BrugerX, så logger på ITSystemY, sker følgende.

1. BrugerX tilgår ITSystemY, via en webbrowser eller App
2. BrugerX vælger, at hun er ansat i ” XXX Kommune”, og dette valg gemmes (f.eks. i en cookie)
3. Systemet initierer et kald fra BrugerX’s app/browser til kommunernes IDP (AD FS server)
4. BrugerX autentikeres på kommunernes IDP med hendes AD brugernavn og password samt evt. 2-faktor validering.
5. Kommunes IDP udsteder herefter et SAML token, som indeholder CLAIMS med eksempelvis følgende oplysninger:

   BrugerX’s navn
   BrugerX’s E-mail Adresse
   BrugerX’s Adgangsgivende roller. (”ITSystemY_Brugere”,”ITSystemY_sagsområde1”)
6. BrugerX’s browser eller app viderestilles retur til it-systemets føderationsserver, hvor SAML token valideres.
7. Hvis token validerer korrekt, læser et script indholdet i CLAIMS, og sikrer at BrugerX’s evt. brugerprofil i it-løsningen oprettes/vedligeholdes, således at Dorthes oplysninger (navn, e-mail mv.) er opdaterede og korrekte, og at BrugerX tildeles de 2 roller
8. BrugerX er nu logget på, og har nu de rettigheder, som den/de pågældende roller giver adgang til.

Eksempel på Assertion i et Claim

```
<Assertion>
           <Issuer>https://sso.sonderborg.dk</Issuer>
           <Signature>
           ... en XMLDSIG signatur, der beviser at tokenet kommer
           ... fra Kommunens AD FS
           </Signature>
           <Subject>
              <NameID>BrugerX@sonderborg.dk</NameID>
           </Subject>
           <AttributeStatement>
                  <Attribute Name="navn">
                       <AttributeValue>Bruger Xander</AttributeValue>
                  </Attribute>
                  <Attribute Name="email">
                       <AttributeValue>BrugerX@sonderborg.dk</AttributeValu
                       e>
                  </Attribute>
                  <Attribute Name="roller">
                     <AttributeValue>ItSystemY_Sagsområde1</AttributeValue>
                     <AttributeValue>ItSystemY_Bruger</AttributeValue>
                  </Attribute>
           </AttributeStatement>
</Assertion>
```

MFA (Multi factor authentication)

I kommunerne anvendes MFA til SSO-løsninger, hvor det vurderes nødvendigt ud fra risikovurderinger og generelt setup.

Som udgangspunkt gælder reglerne, at tilgås et SSO-baseret IT-system fra et ikke-sikret netværk, så vil brugerne blive afkrævet MFA.

Kommer brugeren fra kommunernes interne net, er der som standard ikke noget krav om MFA, medmindre IT-systemet, eller kommunerne kræver dette (f.eks. i forbindelse med NSIS. NSIS= national standard for identiteters sikringsniveau).

I kommunerne anvendes en eller flere af nedstående 2-faktor muligheder:

- OS2Faktor
- MitID
- SoloID
- Microsoft Authenticator
- SMSPasscode
- DUO
- I begrænset omfang FIDO2, via Yubikey

Server-komponenter

Et ADFS Miljø består af to typer servere, ADFS Server (Active Directory Federation Server) og WAP Server. (Web Application Proxy), hvor ADFS er placeret på et internt net, og WAP er placeret i DMZ (demilitarized zone), disse er separeret og sikret via Firewalls.

For Haderslev Kommune sker denne separering ved, at der kun kan opnås adgang fra bestemte IP-adresser.

NSIS

National Standard for Identiteters Sikringsniveauer (NSIS) (https://digst.dk/it-loesninger/standarder/nsis/)

NSIS er et tillidsrammeværk, som gennem tekniske og organisatoriske krav samt governance etablerer et grundlag for tillid til digitale identiteter i national kontekst, og er en del af MitID- og NemLog-in3-løsninger. (https://digst.dk/it-loesninger/nemlog-in/anvendelse/nsis-standarden/)

Selve anvendelsen af NSIS ”IDP” stiller en del flere krav til alle parter, da der her er flere regler og processer, som skal overholdes.

NSIS tillader flere sikringsniveauer LOA (Level of Assurance) pt. Lav, Betydelig og Høj. De forskellige niveauer er beskrevet ved digitaliseringsstyrelsen og kan ses her.

(https://digst.dk/media/21945/vejledning-til-valg-af-sikringsniveau-for-tjenesteudbydere- 202.pdf)

Kommunernes NSIS Setup er baseret på OS2Faktor eller signaturgruppens løsning. (https://www.os2faktor.dk/docs.html)

https://www.signaturgruppen.dk/forside/solutions-medarbejdere/soloid-authenticator

Kommunernes ADFS-miljø

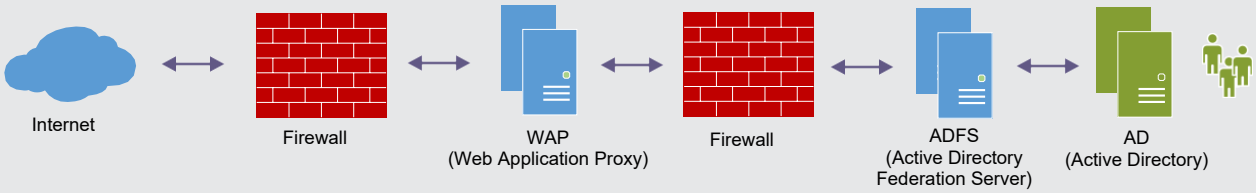
Kommunerne råder i dag over et eller to ADFS-miljøer. I de tilfælde, hvor kommunerne har to miljøer, er de fordelt på et administrativt og et skole/daginstitutions-miljø. De to miljøer er sat op på stort set samme måde, men anvendes af forskellige målgrupper og med henblik på forskellig systemunderstøttelse.

Områderne er koblet op mod hver deres individuelle Active Directory (AD).

Der er ikke etableret Trust mellem disse to AD'er, og miljøerne er separeret via Firewalls.

Alle ADFS-miljøerne er baseret på minimum Windows Server 2019.

Overbliksbillede.



Kommunernes NSIS Miljø

Kommunernes NSIS-miljø er baseret på OS2Faktor eller Signaturgruppen og er sat op som en fælles IDP (Identity Provider):

https://www.os2faktor.dk/docs.html

https://www.signaturgruppen.dk/forside/solutions-medarbejdere/soloid-authenticator

Kommunerne er NSIS godkendt på niveau: **Betydelig**

Azure Single Sign On

Single Sign on gennem Azure kan ske på to måder, enten ved at leverandøren publicerer deres applikation til kommunerne i deres Azure app Gallery, eller via SAML.

Azure App Gallery vejen forgår ved, at leverandøren informerer kommunerne om, hvordan konfigurationen skal foregå, og kommunerne sender enkelte informationer retur, som gør at leve.

På nedstående link ligger der en del information om, hvordan dette forgår i praksis.:
https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-howto-app-gallery-listing

Azure SAML er lidt det samme som ADFS SAML, dog er man her en del mere begrænset i, hvilke muligheder man har, og derfor bruges denne metode sjældent.

Flere info kan findes her:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/auth-saml
https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/saml-toolkit-tutorial