OS2indberetning

SAML opsætning

Version: 1.0.0
Date: 05.03.2020
Author: PSO

Indhold

1 Indledning

Dette dokument er rettet mod teknikere der skal opsætte og konfigurere kommunens AD FS, så det er muligt for kommunens medarbejdere at logge på OS2indberetning.

Dokumentet er primært rettet mod opsætning i AD FS, men indeholder også de nødvendige oplysninger til at en integration kan udføres fra en vilkårligt SAML Identity Provider.

Det forudsættes at læseren har kendskab til konfiguration af AD FS (eller tilsvarende SAML Identity Provider).

1.1 Nødvendige oplysninger

OS2indberetning skal have følgende oplysninger om brugere når de logger på

- Brugerens CPR-nummer
- Brugerens email
- Brugerens roller i OS2indberetning

2 Opsætning af Relying Party i AD FS

For hver OS2indberetning løsning som kommunen anvender (kørsel, ferie), skal der oprettes en ny "Relying Party" i AD FS. Dette gøres på helt normal vis, og metadatafilerne for de 2 løsninger kan hentes her (kommune ændres til kommunens navn):

Kørsel: https://**kommune**-koersel.os2indberetning.dk/Saml2

Ferie: https://**kommune**-ferie.os2indberetning.dk/Saml2

Når disse er oprettet, skal der opsættes relevante "Claim Rules", der sikrer at de relevante oplysninger om brugeren sendes til OS2indberetning på login tidspunkt.

For begge løsninger skal der oprettes det samme sæt af claim rules.

2.1 Opret Claim Rule for CPR

Efter at en Relying Party oprettes i AD FS, åbnes skærmbilledet til Claim Rules automatisk, men man kan også få skærmbilledet frem ved at højreklikke på den Relying Party man har oprettet, og så vælge "Edit Claim rules…"

I dette skærmbillede trykker man på "Add Rule" for at oprette en ny Claim Rule.

I efterfølgende skærmbillede vælges "Send LDAP Attribute as Claims".

Efterfølgende mappes den attribut der indeholder brugerens CPR-nummer til "Name ID", og opsætningen gemmes.

2.2 Opret Claim Rule for Email

Opret endnu en "Send LDAP Attribute as Claims" regel.

Efterfølgende mappes den attribut der indeholder brugerens email (typisk "E-Mail Addresses" fra Active Directory store) til "E-Mail Address", og opsætningen gemmes.

2.3 Opret Claim Rules for roller

Rollerne kan f.eks. hentes fra OS2rollekatalog eller AD-gruppemedlemskab.

2.3.1 Roller fra OS2rollekatalog

Det forudsættes at AD FS plugin'et RoleCatalogueAttributeStore er installeret.

Der oprettes en "custom" claim rule, som indeholder følgende:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 => issue(store = "RoleCatalogueAttributeStore", types = ("roles"), query =
"getSystemRoles", param = c.Value, param = "os2indberetning");
```

2.3.2 Roller fra AD gruppemedlemskab.

Dette claim skal kun tilføjes hvis man ikke har tilføjet roller fra OS2rollekatalog jf. ovenstående. OS2indberetning har pt. Kun én rolle, så der skal kun tilføjes ét gruppemedlemskab.

Tilføj et claim, denne gang med skabelonen "Send Group Membership as a Claim"

Angiv hvilken gruppe brugeren skal være medlem af for at være administrator i OS2indberetning.

Angiv "roles" i "Outgoing claim type".

Angiv "administrator" i "Outgoing claim value".