SOFD Core

SAML opsætning

Version: 1.0.0
Date: 11.09.2019
Author: BSG

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 SOFD Core.

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

SOFD Core skal have følgende oplysninger om brugere når de logger på

- Brugerens identitet (sAMAccountName fra AD)
- Brugerens roller i SOFD Core

Et udklip af de relevante elementer fra et SAML token vises nedenfor – hvis man ikke anvender AD FS kan dette bruges som målbillede for hvad man skal have konfigureret. AD FS brugere kan følgende nedenstående vejledning for at opnå det samme. De 3 mulige roller er vist i eksemplet nedenfor

```
<Subject>
    <NameID>bsg</NameID>
</Subject>
<AttributeStatement>
    <Attribute Name="roles">
        <AttributeValue>admin</AttributeValue>
        <AttributeValue>write</AttributeValue>
        <AttributeValue>read</AttributeValue>
    </Attribute>
</AttributeStatement>
```

2 Opsætning af Relying Part i AD FS

Der skal oprettes en ny ”Relying Party” i AD FS. Dette gøres på helt normal vis, og metadatafilen kan hentes her (kommune ændres til kommunens navn)

https://kommune.sofd.io/saml/metadata

Når denne er oprettet, skal der opsættes relevante ”Claim Rules”, der sikrer at de relevante oplysninger om brugeren sendes til SOFD Core på login tidspunkt.

2.1 Opret Claim Rule for NameID

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 SAM-Account-Name til ”Name ID”, og opsætningen gemmes.

2.2 Opret Claim Rules for roller

Der skal tilføjes én ekstra claim rule til AD FS opsætningen, og den skal hente brugerens roller fra OS2rollekatalog, hvor disse administreres.

Dette gøres ved at oprette 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 = "sofdcore");
```