OS2compliance

SAML opsætning

**Version**: 1.0.1

**Date**: 06.11.2023

**Author**: KBP

Indhold

[1 Indledning 3](#_Toc149577657)

[1.1 Nødvendige oplysninger 3](#_Toc149577658)

[2 Opsætning af Relying Part i AD FS 3](#_Toc149577659)

[2.1 Opret Claim Rule for NameID 4](#_Toc149577660)

[2.2 Opret Claim Rules for roller 4](#_Toc149577661)

[3 Opsætning i OS2rollekatalog 4](#_Toc149577662)

# 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 OS2compliance.

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).

## Nødvendige oplysninger

OS2compliance skal have følgende oplysninger om brugere når de logger på

* Brugerens fkOrg uuid
* Brugerens roller i OS2compliance

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 mulige roller er vist i eksemplet nedenfor

Alternativ til X509SubjectName kan NameId sendes i urn:oasis:names:tc:SAML:2.0:nameid-format:persistent format, indholdet skal så være fkOrgs bruger uuid.

<Subject>

<NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">C=DK,O=123456,CN=Et Navn.,Serial=FKORG-USER-UUID</NameID>

<AttributeStatement>

<Attribute Name="roles">

<AttributeValue>adgang</AttributeValue>

<AttributeValue>administrator</AttributeValue>

</Attribute>

</AttributeStatement>

# Opsætning af Relying Party 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.os2compliance.dk/saml/metadata>

Når denne er oprettet, skal der opsættes relevante ”Claim Rules”, der sikrer at de relevante oplysninger om brugeren sendes til OS2compliance på login tidspunkt.

## 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 Claims Using a Custom Rule”.

**Regel: Hent NameId fra rollekataloget**

c1:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => add(store = "RoleCatalogueAttributeStore", types = ("http://rollekatalog.dk/nameid"), query = "getNameID", param = c1.Value);

## Opret Claim Rules for roller

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

Dette gøres ved at oprette to ”custom” claim rules, som indeholder følgende

**Regel 1 – hent roller fra rollekataloget**

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => issue(store = "RoleCatalogueAttributeStore", types = ("roles"), query = "getSystemRoles", param = c.Value, param = "os2compliance");

**Regel 2 – send roller til OS2compliance**

c:[Type == "rollekatalog:roller"]

=> issue(Type = "dk:gov:saml:attribute:Privileges\_intermediate", Value = c.Value);

# Opsætning i OS2rollekatalog

I OS2rollekatalog kan man manuelt opsætte OS2compliance som et it-system, men det nemmeste er at oprette det som et abonnement. Dette gøres på følgende måde

**1 – opret et SAML it-system**

Under it-systemer vælges ”Opret SAML integration”, og der udfyldes med ”OS2compliance” under System ID på it-systemet som vist nedenfor

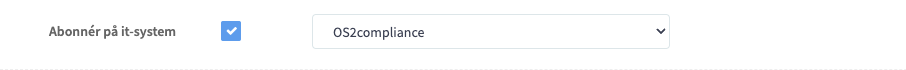
Graphical user interface, text, application, chat or text message

Description automatically generatedA screenshot of a computer

Description automatically generated

**2 – tilføj abonnement**

På redigeringssiden for it-systemet, sættes hak i ”Abonner på it-system”, og så vælges OS2compliance



**3 – vent op til 15 minutter og opret så Jobfunktionsroller**

Der kan gå op til 15 minutter før data er opfrisket, og alle systemroller er hentet ind. Dernæst kan de puttes i Jobfunktionsroller og tildeles til medarbejdere.