OS2autoproces

SAML opsætning for regioner

**Version**: 1.0.0

**Date**: 26.03.2019

**Author**: BSG

Indhold

[1 Indledning 3](#_Toc490221876)

[1.1 Nødvendige oplysninger 3](#_Toc490221877)

[2 Opsætning af Relying Part i AD FS 3](#_Toc490221878)

[2.1 Opret Claim Rule for NameID og email attributterne 3](#_Toc490221879)

[2.2 Opret Claim Rules for roller 5](#_Toc490221880)

[2.2.1 Anvend AD sikkerhedsgrupper til at repræsentere roller 5](#_Toc490221881)

[2.2.2 Anvend Rollekataloget 8](#_Toc490221882)

[3 Registrering af jeres AD FS i Kravmotoren 10](#_Toc490221883)

# Indledning

Dette dokument er rettet mod teknikere der skal opsætte og konfigurere regionernes AD FS, så det er muligt for kommunens medarbejdere at logge på OS2autoproces.

Bemærk at løsningen oprindeligt er udviklet til kommunerne, og deres login foregår via den fælleskommunale login løsning. Derfor er rammerne for AD FS opsætningen lidt firkantede (de er lavet så de matcher kommunernes fælles infrastruktur, så begge login løsninger kan anvendes til OS2autoproces, uden de store gnidninger).

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

OS2autoproces har brug for følgende oplysninger om brugeren, der skal medsendes på login tidspunkt som claims via AD FS

* Brugerens identitet
* Brugerens e-mailadresse
* Brugerens roller

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.

<Subject>

<NameID>

**C=DK,O=20688092,CN=Hans Jensen,Serial=ccbfcb66-af20-407a-809f-52dfa7a835cc**

</NameID>

</Subject>

<AttributeStatement>

<Attribute Name=**"email"**>

<AttributeValue>**bsg@digital-identity.dk**</AttributeValue>

</Attribute>

<Attribute Name=**"urn:roles"**>

<AttributeValue>

**http://os2autoproces.eu/roles/usersystemrole/superuser/1**

</AttributeValue>

</Attribute>

</AttributeStatement>

# Opsætning af Relying Part i AD FS

Der skal oprettes en ny ”Relying Party” i AD FS. Dette gøres på helt normal vis, og OS2autoproces metadatafil kan hentes her

https://www.os2autoproces.eu/saml/metadata

Når denne er oprettet, skal der opsættes relevante ”Claim Rules”, der sikrer at de relevante oplysninger om brugeren sendes til Kravmotoren 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…”

NameID har et specielt (og krævet) format, som stammer fra kommunernes login infrastruktur. I formatet er brugerens unikke ID enkodet under den attribut der hedder ”Serial”. Nedenstående er et eksempel på et lovligt NameID

C=DK,O=20688092,CN=Hans Jensen,Serial=ccbfcb66-af20-407a-809f-52dfa7a835cc

Værdien ”Serial” er den vigtige, da den indeholder brugerens unikke ID, som skal medsendes med præcis samme værdi ved hvert login.

Det er også vigtigt at selve formatet af NameID attributten sættes til

urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName

Ellers vil login ikke fungere.

Én måde at opbygge denne streng på, er via følgende to custom claim rules

**Claim rule 1 – hent sAMAccountName**

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]

=> add(store = "Active Directory", types = ("samaccountname"), query = ";sAMAccountName;{0}", param = c.Value);

**Claim rule 2 – udsted NameID**

c:[Type == "samaccountname"]

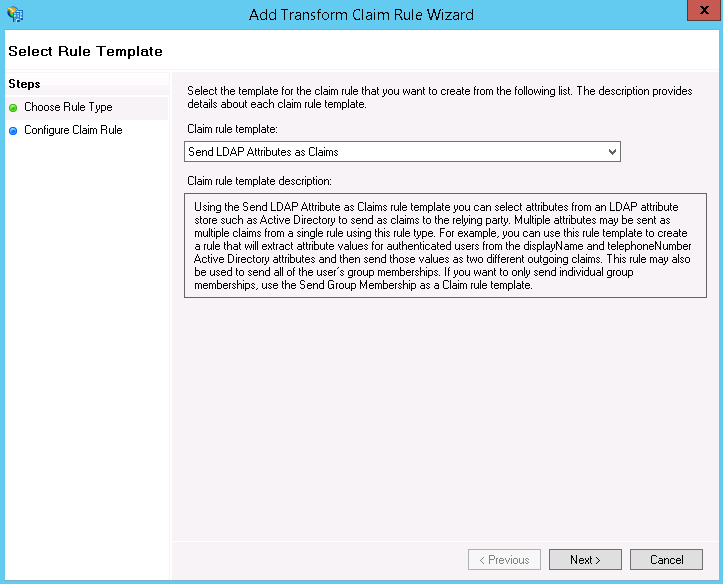
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Value = "C=DK,O=12345678,CN=" + c.Value + ",Serial=" + c.Value, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName");

I ovenstående regel, bør man rette O=12345678 til at matche ens eget CVR nummer.

## Opret Claim Rule for email

Opret endnu en claimrule (højreklik og vælg ”Edit Claim rules...”. I det skærmbillede der kommer frem, trykker man på ”Add Rule” for at oprette en ny Claim Rule.

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



Efterfølgende mappes E-Mail-Addresses til et udgående claim med værdien ”email”.

## Opret Claim Rules for roller

Der er 2 roller i OS2autoproces, men de er ikke nødvendige for at foretage et login til løsningen. De to roller er tiltænkt superbrugere, der skal kunne se processer på tværs af kommunen. En lokal superbruger er begrænset til at kunne se processer fra egen afdeling, hvor en ”fuld” superbruger kan se for hele regionen.

Alle brugere der logger på løsningen kan se egne processer, samt de processer der er gjort offentlige, uagtet om de er tildelt en rolle eller ej.

Det claim der skal sendes hedder ”urn:roles”, og kan enten udelades, eller indeholde en af følgende to værdier

* **http://os2autoproces.eu/roles/usersystemrole/local\_superuser/1**
* **http://os2autoproces.eu/roles/usersystemrole/superuser/1**

Ovenstående navnestandard stammer fra kommunernes logininfrastruktur, men er blot ”rolle-id’er”, og der er ikke enkodet noget specielt i dem, og de skal blot behandles som tekst-strenge.

Om man ønsker at bruge AD grupper, eller et andet IdM værktøj til at styre rollerne, er op til den enkelte region.