Kravmotoren

SAML opsætning

Version: 1.0.1
Date: 22.09.2017
Author: BSG

Indhold

1 Indledning 3
1.1 Nødvendige oplysninger 3
2 Opsætning af Relying Part i AD FS 3
2.1 Opret Claim Rule for NameID og email attributterne 3
2.2 Opret Claim Rules for roller 5
2.2.1 Anvend AD sikkerhedsgrupper til at repræsentere roller 5
2.2.2 Anvend Rollekataloget 8
3 Registrering af jeres AD FS i Kravmotoren 10

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 Kravmotoren.

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

Kravmotoren skal have følgende oplysninger om brugere når de logger på

- Brugerens identitet (vises i brugergrænseflade, og kommer i loggen når brugerens udfører handlinger der skal logges)
- Brugerens e-mailadresse (vil på sigt blive anvendt til at sende notifikationer)
- Brugerens roller i Kravmotoren

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>bsg</NameID>
</Subject>
<AttributeStatement>
    <Attribute Name="email">
        <AttributeValue>bsg@digital-identity.dk</AttributeValue>
    </Attribute>
    <Attribute Name="urn:dk:kravmotoren:roles">
        <AttributeValue>http://kravmotoren.dk/editor</AttributeValue>
        <AttributeValue>http://kravmotoren.dk/purchaser</AttributeValue>
    </Attribute>
</AttributeStatement>
```

2 Opsætning af Relying Part i AD FS

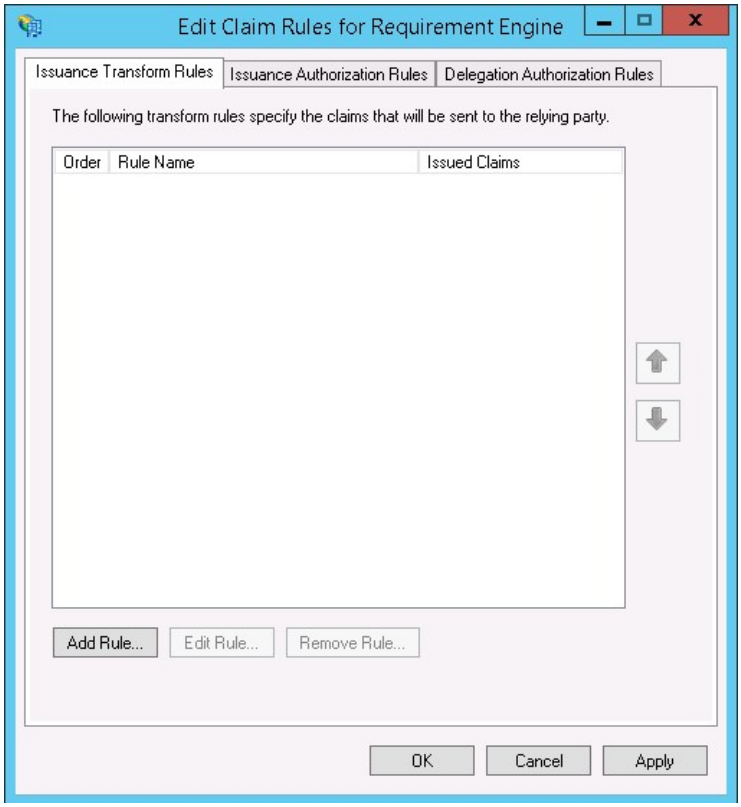
Der skal oprettes en ny ”Relying Party” i AD FS. Dette gøres på helt normal vis, og Kravmotorens metadatafil kan hentes her

https://www.os2kravmotor.dk/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.

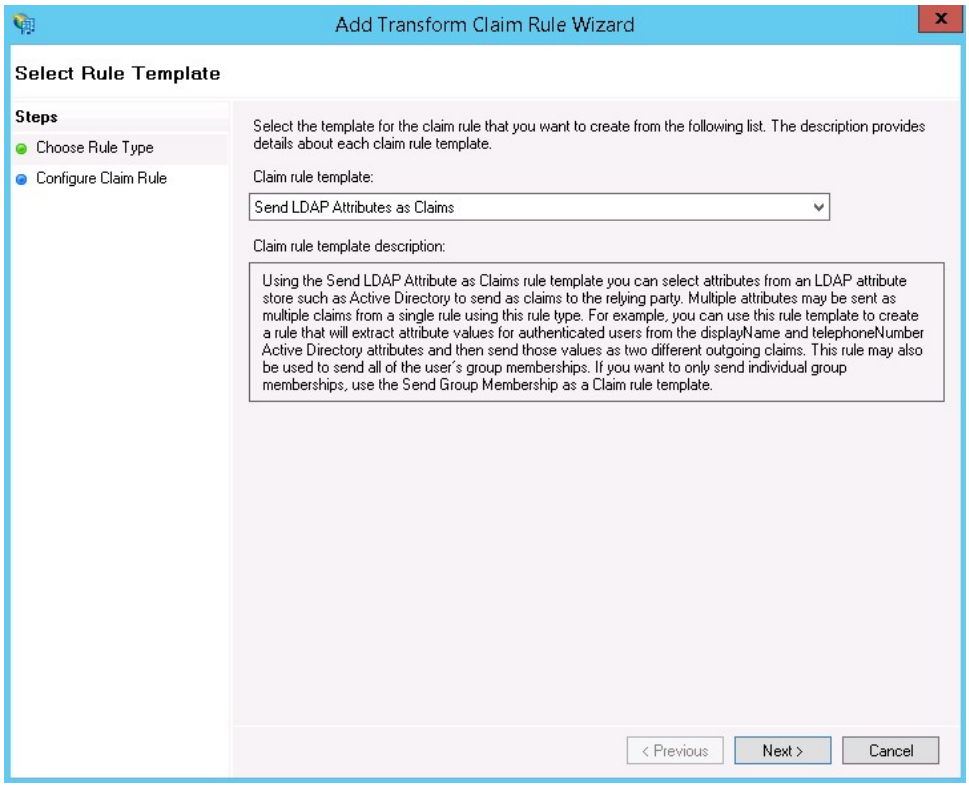
2.1 Opret Claim Rule for NameID og email attributterne

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…”

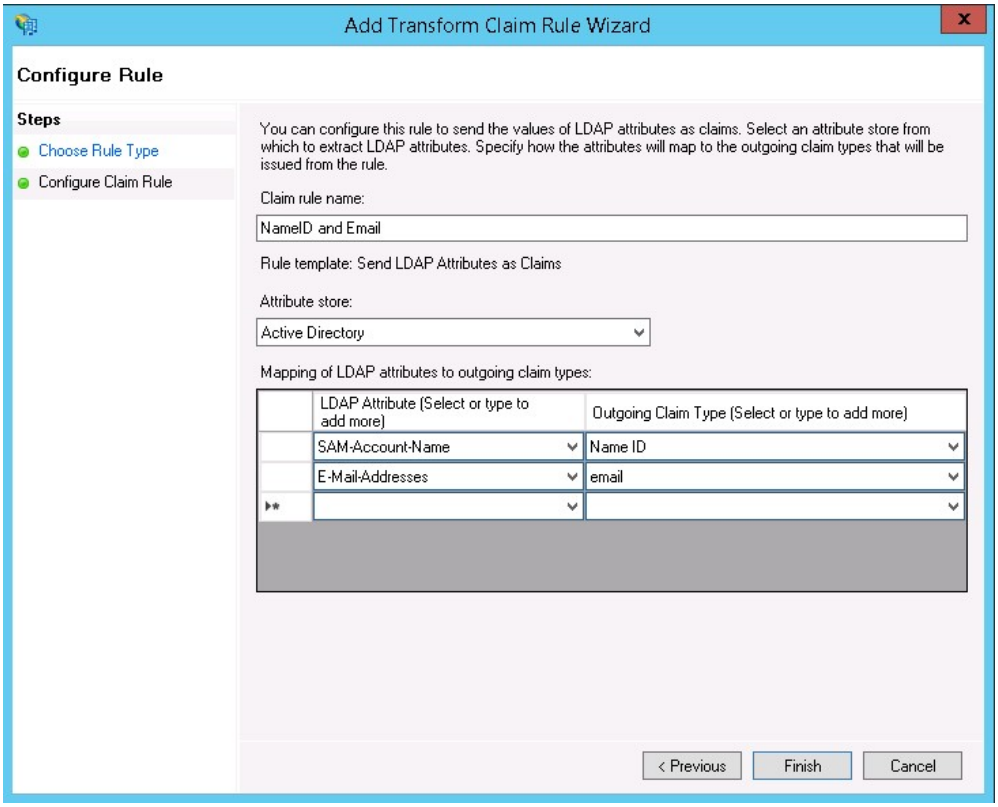


I dette skærmbillede trykker man på ”Add Rule” for at oprette en ny Claim Rule.

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



Efterfølgende mappes SAM-Account-Name og E-Mail-Addresses til de udgående claims, ved at udfylde skærmbilledet så det ligner nedenstående



Herefter er brugerens identitet og email adresse mappet korrekt.

2.2 Opret Claim Rules for roller

Der er forskellige måder at håndtere rolle-tildeling. Nedenfor er beskrevet 2 forskellige scenarier, som er de mest almindelige. Vælg den metode der passer bedst til jeres kommune.

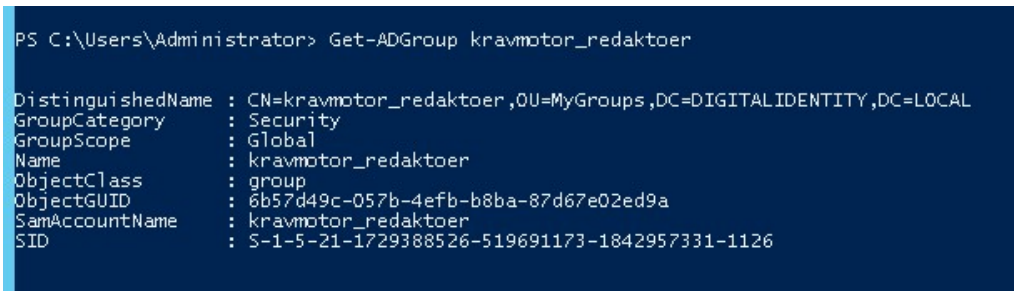
2.2.1 Anvend AD sikkerhedsgrupper til at repræsentere roller

Hvis man ønsker at bruge AD sikkerhedsgrupper til at styre hvilke roller som ens medarbejdere har i Kravmotoren, så skal man starte med at oprette 3 sikkerhedsgrupper i AD, og fremsøge deres SID.

De 3 roller der anvendes i Kravmotoren, og som der skal oprettes grupper for, hedder

- Redaktør
- Indkøber
- Administrator

Hvis man åbner Powershell, kan man aflæse SID på en sikkerhedsgruppe ved at bruge kommandoen Get-ADGroup. Nedenfor er vist et skærmbillede hvor der er lavet et opslag på sikkerhedsgruppen "kravmotor_redaktoer". Erstat dette med de navne som sikkerhedsgrupperne har fået i jeres AD. Noter SID værdierne, vi skal bruge dem i AD FS opsætningen.



Inde i AD FS skal vi nu oprette 3 Claim Rules, en for hver rolle. Dette gøres på følgende måde for hver rolle

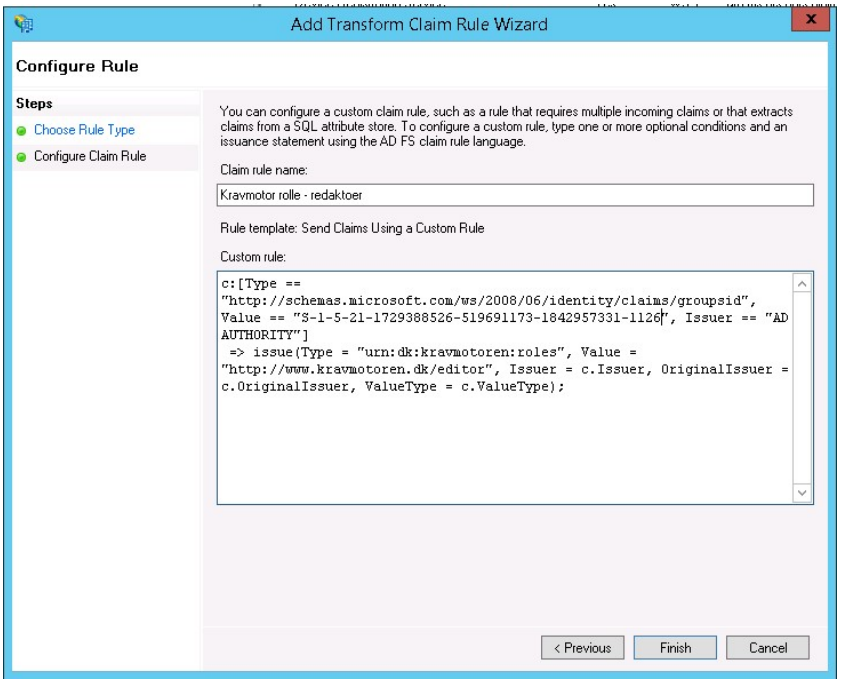
1. Tilføj en ny Claim Rule, og vælg typen "Send Claims using Custom Rule".
2. Indtast et navn på Claim Rulen, og indtast følgende regel-streng hvor SID strengen og rolle-navnet tilpasses

```
   c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
     Value == "S-1-5-21-1729388526-519691173-1842957331-1126",
    Issuer == "AD AUTHORITY"]
 => issue(Type = "urn:dk:kravmotoren:roles",
          Value = "http://kravmotoren.dk/editor",
         Issuer = c.Issuer,
OriginalIssuer = c.OriginalIssuer,
     ValueType = c.ValueType);
```

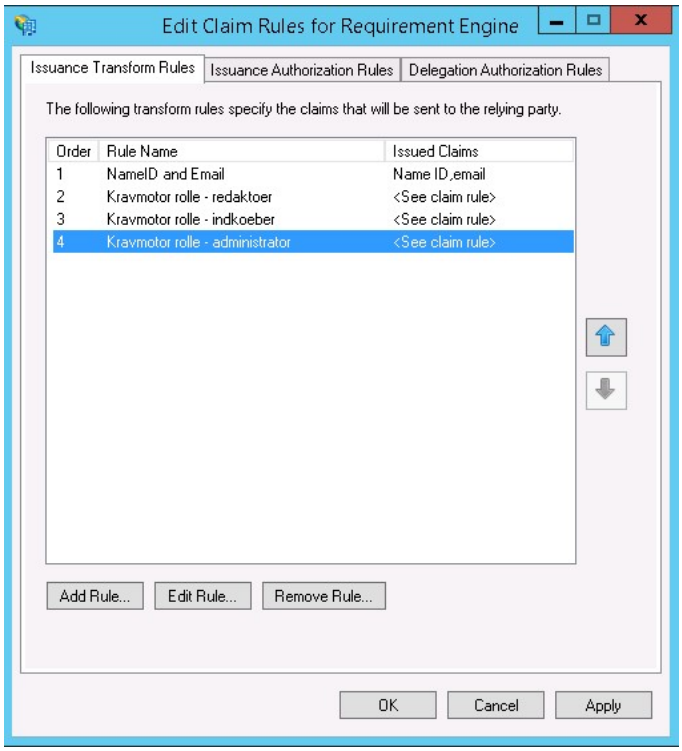
I ovenstående vil det være 2. linje der indeholder SID værdien som skal erstattes med den SID værdi som den tilhørende sikkerhedsgruppe har i jeres AD, og 5. linje som indeholde rolle-navnet. De 3 rollenavne er

- Redaktør => http://kravmotoren.dk/editor
- Indkøber => http://kravmotoren.dk/purchaser
- Administrator => http://kravmotoren.dk/admin

Nedenstående skærmbillede viser hvordan reglen ser ud i AD FS.



Når alle 3 roller er oprettet, vil listen over Claim Rules se cirka sådan her ud



2.2.2 Anvend Rollekataloget

Hvis man anvender Rollekataloget er de nødvendige roller oprettet i Rollekataloget, og der skal blot oprettes 3 Claim Rules i AD FS til at hente medarbejdes roller. Disse 3 Claim Rules skal oprettes som typen ”Send Claims using Custom Rule”, og de regler der skal oprettes er

Regel 1 – konfiguration af it-system

```
=> add(Type = "http://rollekatalog.dk/itsystem",
      Value = "Kravmotoren");
```

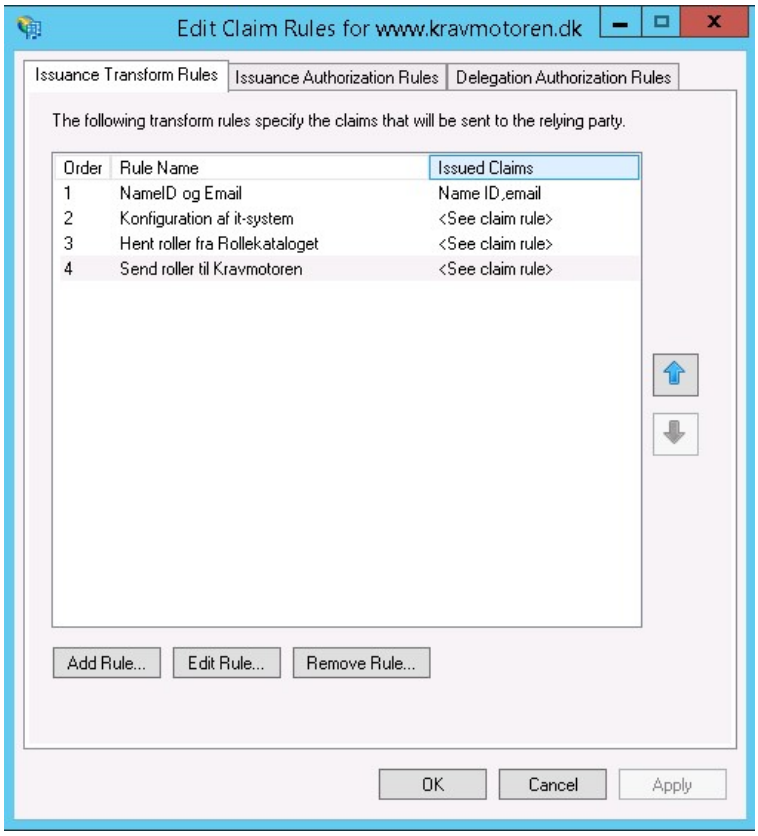
Regel 2 – hente brugerens roller fra Rollekataloget

```
c1:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
  Issuer == "AD AUTHORITY"]
 && c2:[Type == "http://rollekatalog.dk/itsystem"]
 => add(store = "RoleCatalogueAttributeStore",
        types = ("http://rollekatalog.dk/oio-bpp"),
        query = "systemroles",
        param = c1.Value,
        param = c2.Value);
```

Regel 3 – sende brugerens roller til Kravmotoren

```
c:[Type == "http://rollekatalog.dk/oio-bpp"]
 => issue(Type = "urn:dk:kravmotoren:roles",
        Issuer = c.Issuer,
OriginalIssuer = c.OriginalIssuer,
         Value = c.Value,
Properties["http:/
/schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:basic", Properties["http://schemas.
xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = "Privileges");
```

Når man har oprettet alle 3 roller, vil ens list af Claim Rules se nogenlunde sådan her ud



3 Registrering af jeres AD FS i Kravmotoren

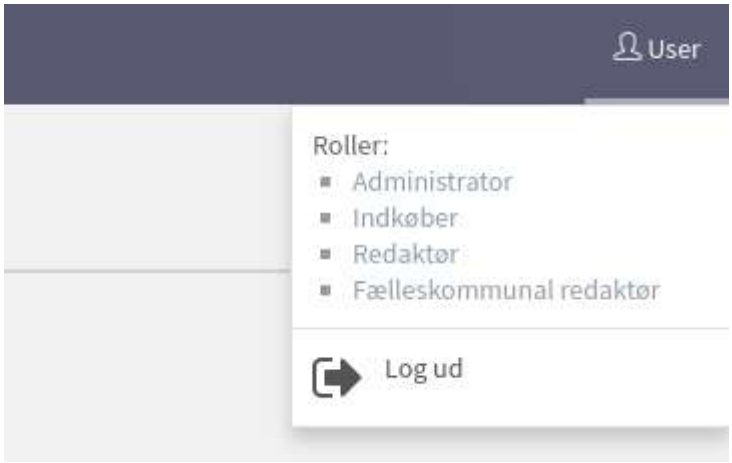
Jeres AD FS skal registreres i Kravmotoren før brugerne kan gennemføre et login. Dette kræver at I sender enten URL adressen på hvor man kan hente jeres metadata (foretrukken metode), eller at I downloader den selv, og sender filen.

URL eller fil skal sendes til bsg@digital-identity.dk

Efter registreringen er foretaget, kan I forsøge et login her

https://www.os2kravmotor.dk/

Når I er logget på, vil man kunne se ens brugernavn i højre øverste hjørne, og ved at klikke her, folder der sig en menu ud, hvor man kan se hvilke roller man er tildelt. På den måde kan I verificere at jeres opsætning fungerer som den skal.



Bemærk at rollen "Fælleskommunal redaktør" ikke er en I kan styre via jeres AD FS, men i stedet er en rolle som tildeles centralt, hvilket styres af den fælleskommunale redaktørgruppe. Hvis I har brugere der har brug for denne adgang, så kontakt dem, som så efterfølgende skal kontakte bsg@digital-identity.dk for at få oprettet denne rolle til brugeren.