GLOBETEAM

ADFS Opsætning til Statens SSO Økonomistyrelsen

Globeteam A/S · Virumgårdsvej 17A · DK-2830 Virum · Telefon +45 7026 2970

Indhold

Globeteam A/S · Virumgårdsvej 17A · DK-2830 Virum · Telefon +45 7026 2970

1 Intro

Denne vejledning er udført på en Windows 2019 Server med ADFS-rollen installeret.

ADFS-serveren benytter ikke MFA og i de kommende eksempler skal alle brugere benytte SSO løsning.

Indholdet i dette dokument er udarbejdet for at assistere institutionerne i den korrekte oprettelse af en "Relying Party Trust" med Økonomistyrelsens SSO-løsning.

Dette dokument beskriver, hvad en institution skal gøre for at blive tilkoblet

Økonomistyrelsens single sign-on-løsning (Statens SSO). Institutionen har i dette tilfælde rollen identitet udbyder overfor Statens SSO – dvs. den skal levere validering af brugere.

1.1 I drift på Statens SSO

Når institutionen er tilkoblet Statens SSO, skal brugerne ikke længere anvende de gamle links til fagsystemerne. I stedet skal brugeren anvende de links til fagsystemerne, som giver adgang via Statens SSO. Oversigt over disse links kan findes her:

https://modst.dk/systemer/systemstandarder/single-sign-on/

Det bemærkes dog, at nogle fagsystemer også giver adgang med single sign-on via en knap på den normale loginside.

1.2 Anbefalinger om certifikater

For at forhindre hyppige ændringer til federationsforbindelserne anbefaler vi at der bruges et certifikat udstedt lokalt fra jeres maskine til både signing og decryption med en længere levetid end den som ADFS opretter som standard.

Vi anbefaler følge til jeres opsætning af certifikatet:

- SHA-256
- Levetid: 3-5 år
- RSA: 4096bits

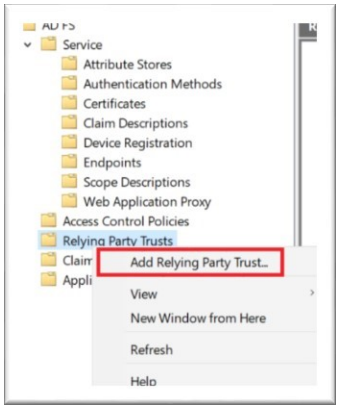
Globeteam A/S · Virumgårdsvej 17A · DK-2830 Virum · Telefon +45 7026 2970

2 How-to guide

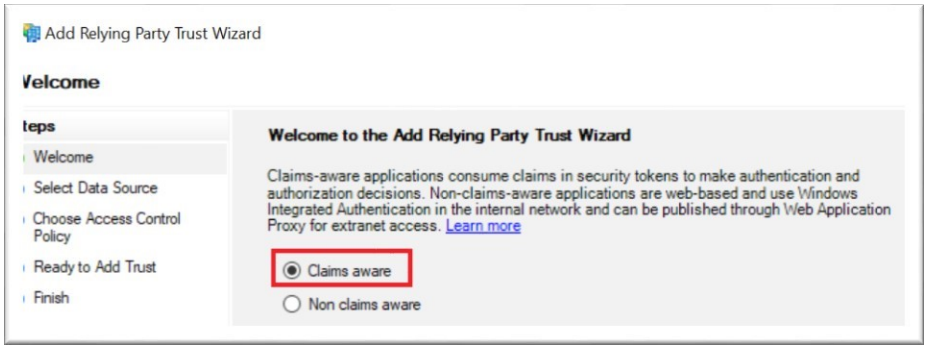
2.1 Opsætning af relying party

Figur 1 I ADFS-konsollen find "Relying parties".

Figur 2 Højreklik og vælge

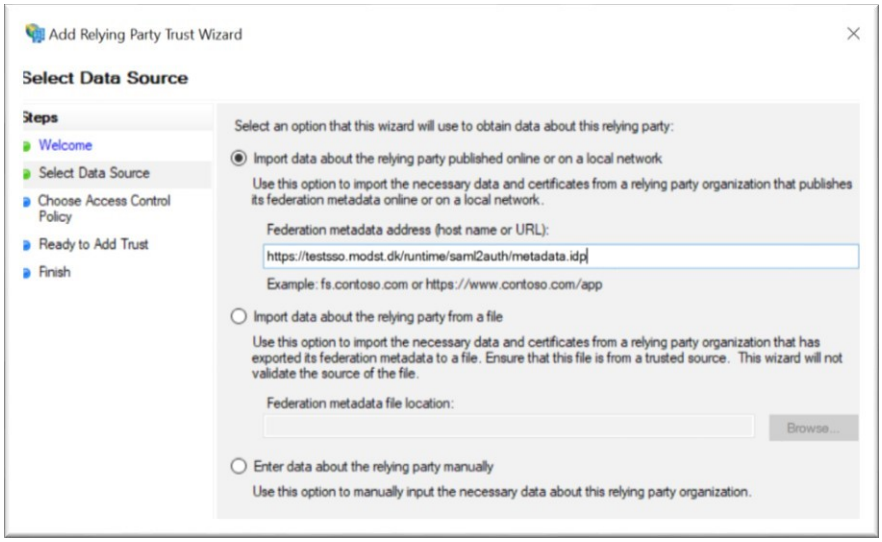


Figur 3 I konfigurationswizard vælg "Claim Aware" og tryk "start"



Globeteam A/S · Virumgårdsvej 17A · DK-2830 Virum · Telefon +45 7026 2970

Figur 4 Indtast xml-datakilden – bemærk der er to miljøer hos ØS, test og prod

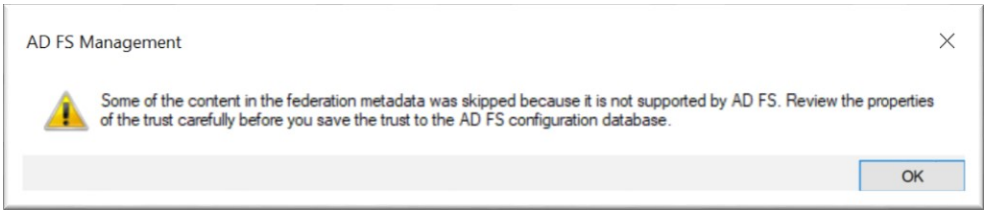


Xml-datakilder – bemærk der er to miljøer hos ØS, test og prod:

Test: https://testsso.modst.dk/runtime/saml2auth/metadata.idp

Prod: https://sso.modst.dk/runtime/saml2auth/metadata.idp

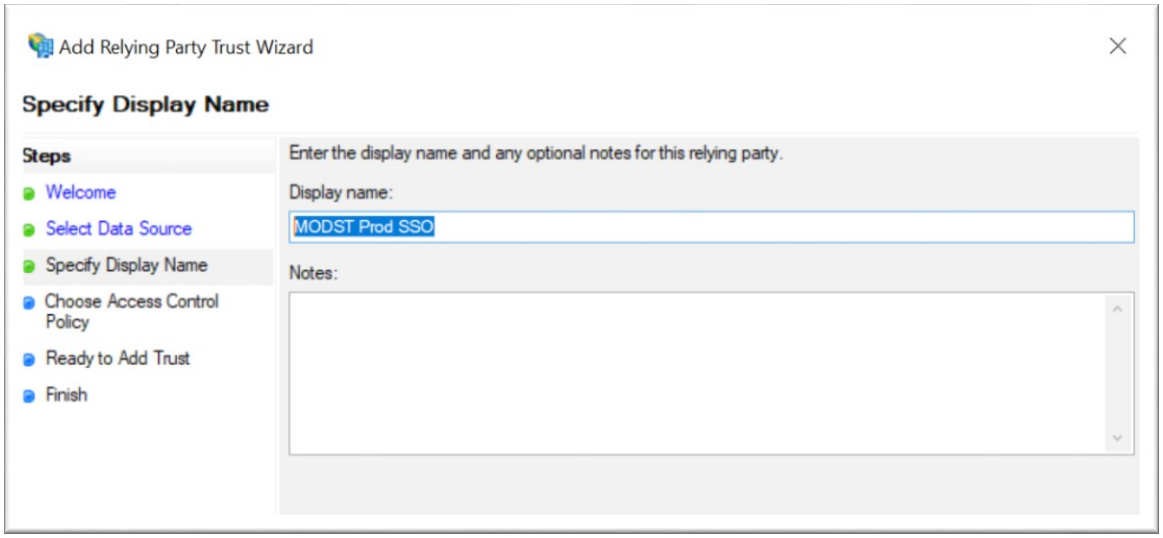
Figur 5 Tryk "Næste" og sig ok til advarslen



- Navngive forbindelsen, eksempelvis:
  Test: MODST Test SSO
  Prod: MODST Prod SSO

Globeteam A/S · Virumgårdsvej 17A · DK-2830 Virum · Telefon +45 7026 2970

Figur 6 Navngiv forbindelsen.

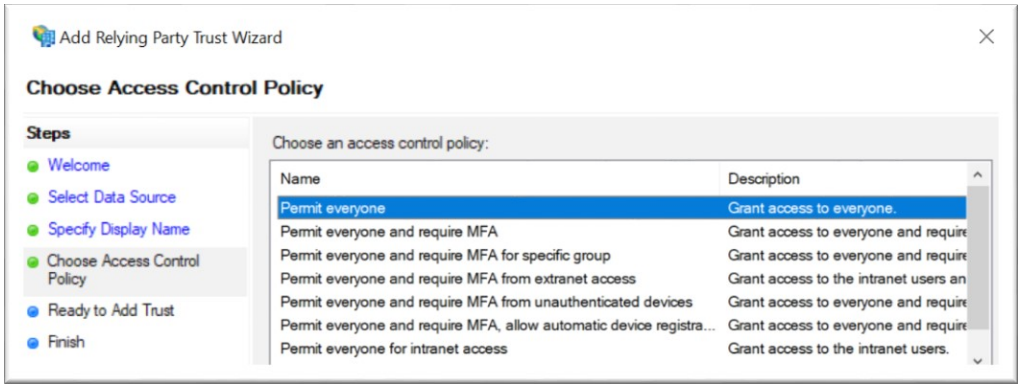


Ved navngivning af forbindelsen anbefales det, at anvende genkendelige navne, eksempelvis:

Test: MODST Test SSO

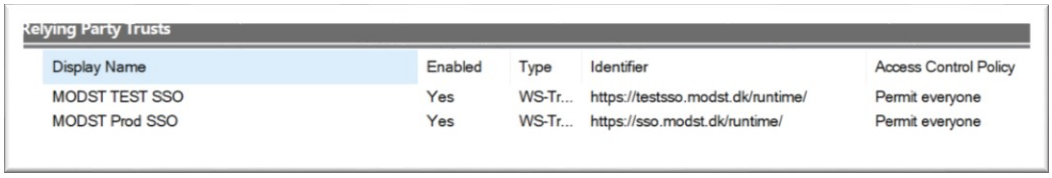
Prod: MODST Prod SSO

Figur 7 Sæt adgangskontrol.



Vælg den adgangspolitik, der passer til jeres eksisterende infrastruktur. Se ”Adgangs kontrol i ADFS” længere nede i dokumentet for en kort forklaring af mulighederne.

Figur 8 Tryk næste indtil de sidste 2 punkter i wizarden afsluttes. Herefter vil du se et skærmbilled med de oprettede Relying Parties.



For opsætning af Claim regler forsæt til afsnit 2.2 Opsætning af LDAP claim rules.

Globeteam A/S · Virumgårdsvej 17A · DK-2830 Virum · Telefon +45 7026 2970

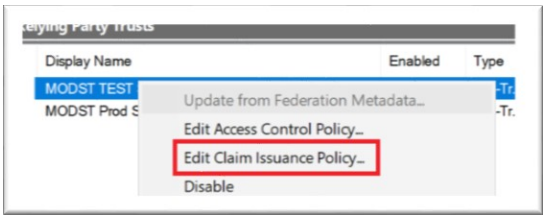
2.2 Opsætning af LDAP claim rules

Følgende guide skal udføres pr. relying party trust. I guiden her lægges LDAP regler direkte på

Relying Party trust. Bemærk, at disse regler kun aktiverer når brugerne logger på via Active Directory. Anvender i andre upstream IdP'er på AD FS til autentificering, så kræver det at disse LDAP regler populeres på den oprindelige IdP.

1) Højre klik på den nye oprettet relying party trust og vælg edit claim issuance policy

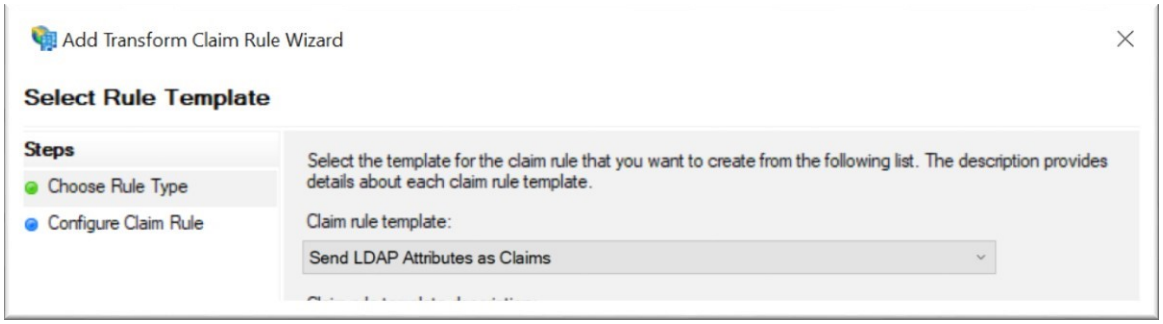
Figur 9 Højreklik-menu på den valgte Relying Party, hvor "Edit Claim Inssurance Policy" er valgt.



Det åbnet vindue bør ikke indholde nogle eksiterende regler.

2) vælg "add rule"
3) Vælg "Send LDAP Attributes as Claims" og tryk næste

Figur 10 Add Transform Claim Rule Wizard - hvor "Send LDAP Attributes as Claims" er valgt



4) Give reglen et navn "LDAP", vælg "Active directory" som datastore og udfyld felterne "LDAP Attribute" og "Outgoing Clam Type". Det er vigtigt at udskifte Outgoing Claim Type med værdierne i tabellen og ikke vælge standardværdierne, som den kan tilbyde via drop down menuen. I nedenstående anvendes mail-attributten på brugerne som brugerid i fagsystemerne (user id og Name claims). Hvis I bruger UPN navn til brugerid, så skal LDAP attributten for user id og Name claim være User-Principal-Name attributten.

Tabel 1 LDAP Regler

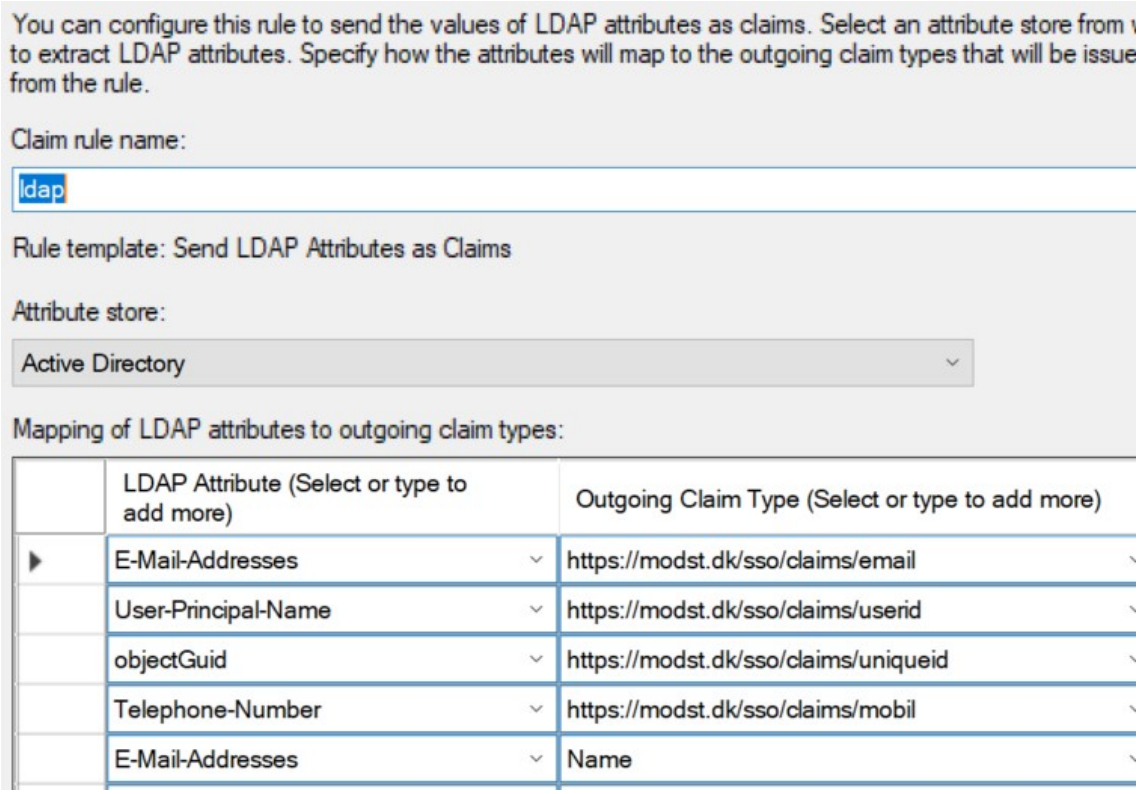
LDAP Attribute	Outgoing Claim Type
E-Mail-Addresses	https://modst.dk/sso/claims/email
E-Mail-Addresses	https://modst.dk/sso/claims/userid
objectGuid	https://modst.dk/sso/claims/uniqueid
Mobile	https://modst.dk/sso/claims/mobile

Globeteam A/S · Virumgårdsvej 17A · DK-2830 Virum · Telefon +45 7026 2970

LDAP Attribute	Outgoing Claim Type
Surname	https://modst.dk/sso/claims/surname
Given-Name	https://modst.dk/sso/claims/givenname
E-Mail-Addresses	Name

NB! Opdateret liste for LDAP-regler kan findes i den tekniske vejledning for opsætning af institution til Statens SSO på Økonomistyrelsens hjemmeside: https://oes.dk/systemer/faelles-systemer-i-staten/data-og-integrationer/single-sign-on/

Figur 11 Navngivning af Claim rule, samt udsnit af LDAP-reglerne.



5) Tryk ”Finish” for at afslutte.

2.3 Opsætning af Custom rules

I dette afsnit vil der blive vist et enkelt eksempel på hvordan der oprettes en ”custom rule” på jeres ADFS Server for de attributter som ikke findes i jeres AD gennem LDAP-reglerne.

Syntaksen i hvert regel er følgende: `=>`
`issue(type = "Claimtype", value = "value");`
Så for CVR vil det se således ud:

```
=> issue(type = "https://modst.dk/sso/claims/cvr", value = "12345678");
```

Det vil være nødvendigt at rette både CVR og assurancelevel værdierne til.

Globeteam A/S · Virumgårdsvej 17A · DK-2830 Virum · Telefon +45 7026 2970

Tabel 2 Specifikation af værdier i assurancelevel

Værdi	Beskrivelse
2	Der er foretaget enkeltfaktor validering, f.eks. brugernavn/adgangskode eller kerberos spnego i forbindelse med en domain joined device
3	Der er foretaget to-faktor validering af brugeren – f.eks. sms kode, nemid eller tilsvarende.

Udfør guiden for hvert af følgende regler: CVR, assurancelevel og logonmethod. Bemærk, at logonmethod claim'en skal populeres efter, hvordan brugerens oprindelige logon er foretaget.

Så hvis brugeren er logget på med tofaktor, så skal logonmethod attributten afspejle dette. Det samme gælder assurancelevel claim'en. Se mere om dette i ØSs generelle tilslutningsvejledning, under afsnittet: "Information om hvilke attributter, institutionen skal medsende fra sin lokale IdP". AD FS afslører sin logonmetode via følgende claim: http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod. Se mere her: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technicalreference/the-role-of-claims.

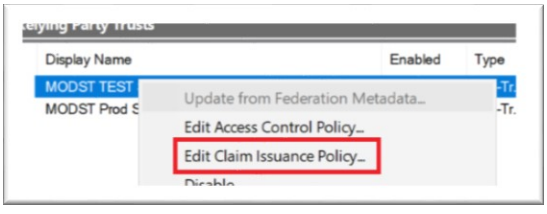
Denne guide er baseret på en AD FS, der anvender forms-login og enkeltfaktor. Derfor 2 i assurancelvel, og username-password-protected-transport. Hvis jeres AD FS anvender kerberos og enkeltfaktor for alle brugere, så skal assurancelevel stå til 2 og logonmethod til kerberosspnego. Hvis AD FS anvendes både internt og eksternt fra, så skal AD FS' authenticationmethod claim oversættes til den tilsvarende logonmethod og assurancelevel claim til at afspejle dette korrekt for hvert login.

Tabel 3 Forskellige claim typer

Claim Type
=> issue(type = "https://modst.dk/sso/claims/cvr", value = "12345678");
=> issue(type = "https://modst.dk/sso/claims/assurancelevel", value = "2");
=> issue(type = "https://modst.dk/sso/claims/logonmethod", value = " username-passwordprotected-transport");

Følgende guide skal udføres pr. relying party trust

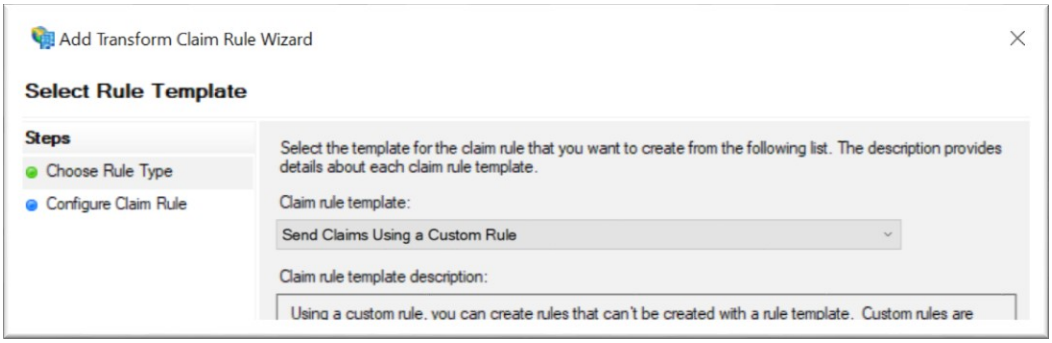
Figur 12 Højre klik på den nye oprettet relying party trust og vælg edit claim issuance policy



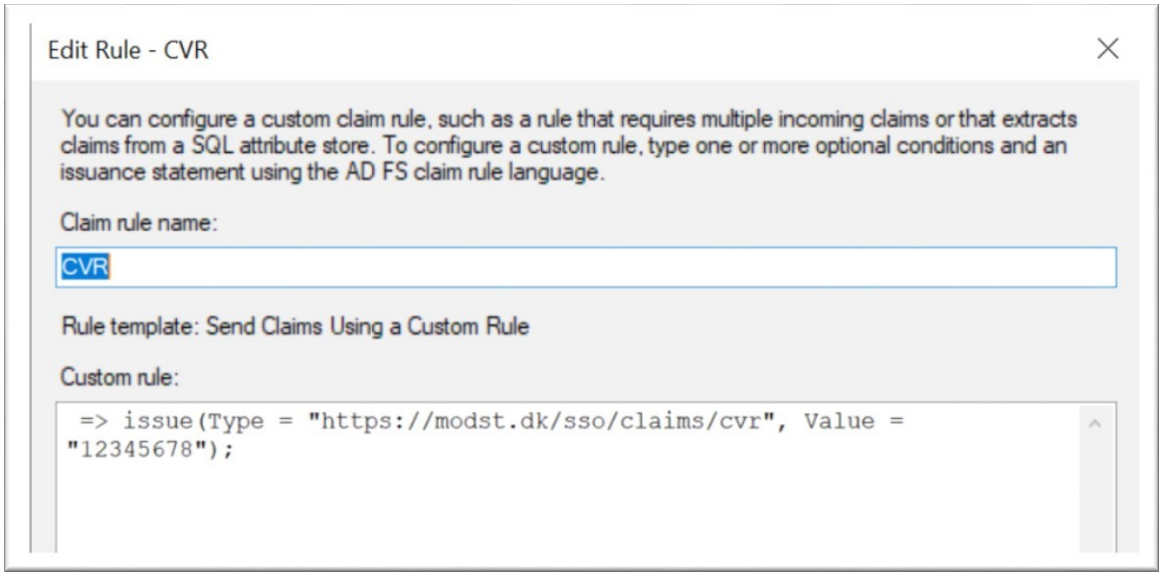
Det åbnede vindue bør ikke indeholde nogle eksisterende regler, vælg "add rule".

Globeteam A/S · Virumgårdsvej 17A · DK-2830 Virum · Telefon +45 7026 2970

Figur 13 Vælg "Send Claims Using a Custom Rule" og tryk næste



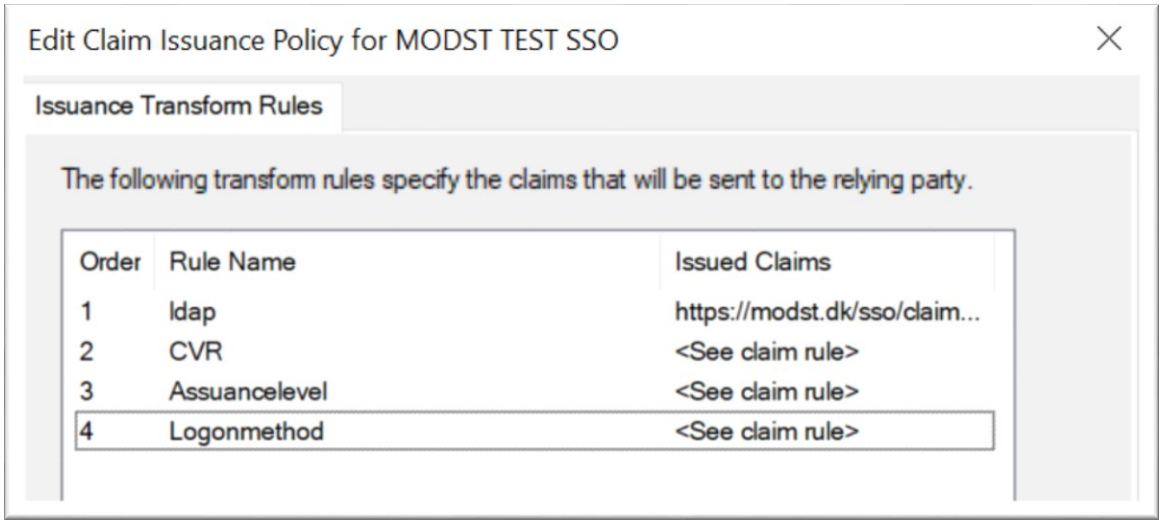
Figur 14 Kopier en regel fra tabellen med LDAP-regler, og indtast som vist i eksemplet (her er for CVR), tryk der efter ok.



Listen med regler findes i Tabel 1 LDAP Regler

Globeteam A/S · Virumgårdsvej 17A · DK-2830 Virum · Telefon +45 7026 2970

Figur 15 Nu burde listen over regler se således ud



2.4 Opsætning af Name ID claim

Name ID er en særskilt claim, som skal tilføjes som den sidste claim regel på Relying Parties.

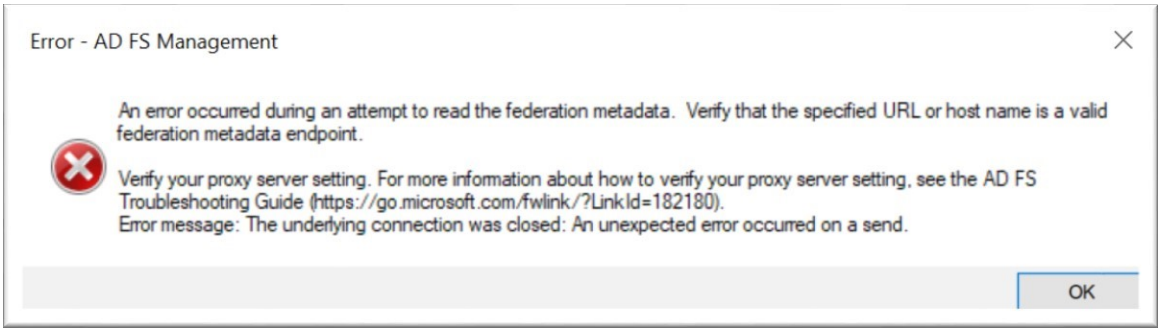
Name ID oversættes fra https://modst.dk/sso/claims/userid claimen som en Transform rule. Denne transform rule skal således transformere userid claimen til en ny claim af typen Name ID (persistent identifier).

Dette afslutter claims opsætningen på Relying Party.

Globeteam A/S · Virumgårdsvej 17A · DK-2830 Virum · Telefon +45 7026 2970

3 Fejlfinding

3.1 Fejl ved hentning af SSO meta data.



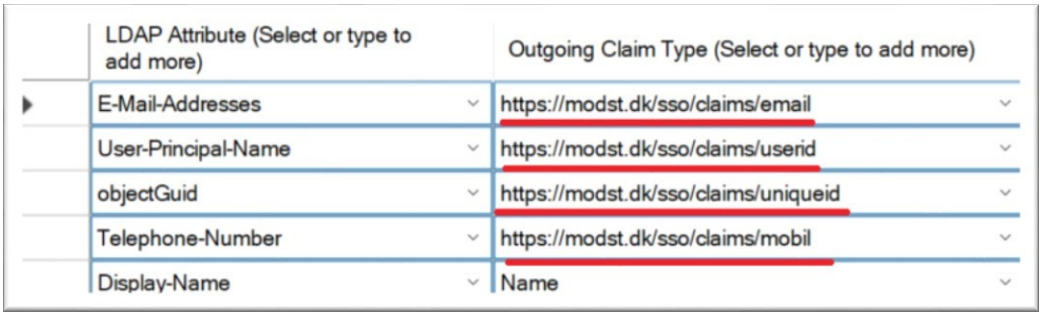
I vores 2016/209 Server labs er dette problem opstået fordi ADFS-servicen forsøger at kommunikere med en standard der er lavere end hvad Statens SSO tillader hvilket er TLS 1.2.

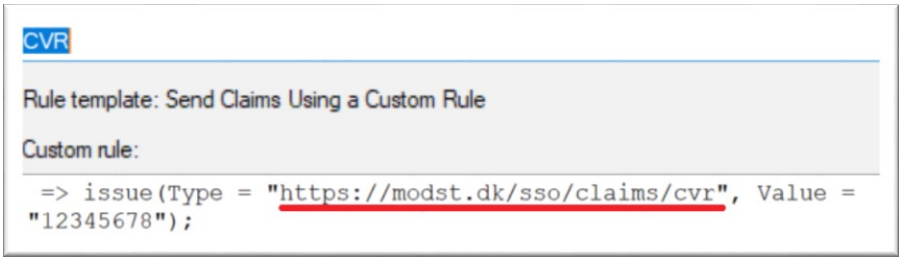
Dette kan løses ved hærdne jeres server til at benytte den korrekt standard.

3.2 "Unable to validate SAML message

Hvis I oplever denne fejl, så skal I validere Claim typen I jeres regler.

Hvis ikke der bliver fremsendt de forventede typer mod Statens SSO, så vil I muligvis få beskeden "Unable to Validate SAML message". Hyppigst er der en fejl i indtastningen af jeres Claim types. Se "Tabel 3 Forskellige claim typer" i afsnit 4 Claim types hos Statens SSO".





Globeteam A/S · Virumgårdsvej 17A · DK-2830 Virum · Telefon +45 7026 2970

4 Claim types hos Statens SSO

Claim	Eksempel værdi	AD Attribute	Beskrivelse
https://modst.dk/sso/claims/email	jodo@myemail.com	E-Mail-Addresses	Brugerens E-mail
https://modst.dk/sso/claims/userid	jodo@myemail.com	User-Principal-Name	Efter aftale med Økonomistyrelsen kan UPN (User Principal Name) anvendes.
https://modst.dk/sso/claims/uniqueid	l1RmJG/LQ0CK7DHvw3pHvw==	objectGuid	Brugerens Unikke ID fra AD i Base64
https://modst.dk/sso/claims/mobil	30123456	mobile	Bruges til 2-trins validering
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	jodo@myemail.com	E-Mail-Addresses	Navnet der evt. præsenteres i applikationer.
https://modst.dk/sso/claims/surname	Doe	Surname	Brugerens efternavn
https://modst.dk/sso/claims/givenname	John	Given-Name	Brugerens fornavn
https://modst.dk/sso/claims/cvr	12345678	-Findes ikke i AD	Institutionens CVRnummer

Claim	Eksempel værdi	AD Attribute	Beskrivelse
https://modst.dk/sso/claims/assurancelevel	2 eller 3	-Findes Ikke i AD	Skal populeres efter om brugeren er logget på med kerberos eller enkeltfaktor forms login (2) eller tofaktor (3)
https://modst.dk/sso/claims/logonmethod	username-password-protectedtransport, Kerberos-spnego eller two-factor	-Findes ikke i AD	Skal populeres efter hvordan brugeren er logget på (kerberos, forms login eller to-faktor.
Name ID (persisten identifier)	Indholdet af https://modst.dk/sso/claims/userid overst til Name ID (persistent identifier)	Findes ikke i AD	Skal oversættes fra userid claim'en til et Name ID (transform rule)