



ADFS Opsætning til Statens SSO Økonomistyrelsen



Indhold

1 Intro	
1.1 l drift på Statens SSO	
1.2 Anbefalinger om certifikater	3
2 How-to guide	4
2.1 Opsætning af relying party	4
2.2 Opsætning af LDAP claim rules	7
2.3 Opsætning af Custom rules	8
3 Fejlfinding	12
3.1 Fejl ved hentning af SSO meta data	12
3.2 -Unable to validate SAML message	12
4 Claim types hos Statens SSO	



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 l 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



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"

Vizard
Welcome to the Add Relving Party Trust Wizard
Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows
Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more
Claims aware
O Non claims aware



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

Select an option that this wizard will use to obtain data about this relying party: Welcome Select Data Source Choose Access Control Policy Ready to Add Trust Finish Finish Contose this point of the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that published online or on a local network. Federation metadata address (host name or URL): https://testsos.modst.dk/runtime/sami2auth/metadata.idpl Example: fs.contosc.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that hu exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will use this option to import the necessary data and certificates from a trusted source. This wizard will use this option to a file.	lect Data Source	
Select Data Source Use this option to import the necessary data and certificates from a relying party organization that puts federation metadata online or on a local network. Choose Access Control Policy Ready to Add Trust Finish Federation metadata address (host name or URL): Intervention Intervention Finish Example: fs.contos.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that he exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard vial date the source of the file.	ps Welcome	Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network
Finish Example: fs.contoso.com or https://www.contoso.com/app Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that he exported ats federation metadata to a file. Ensure that this file is from a trusted source. This wizard v validate the source of the file.	 Select Data Source Choose Access Control Policy Ready to Add Trust Finish 	Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network. Federation metadata address (host name or URL):
		Example: fs.contoso.com or https://www.contoso.com/app O Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.
Federation metadata file location: Brow		Federation metadata file location: Browse Browse

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

Test: <u>https://testsso.modst.dk/runtime/saml2auth/metadata.idp</u> Prod: <u>https://sso.modst.dk/runtime/saml2auth/metadata.idp</u> *Figur 5 Tryk "Næste" og sig ok til advarslen*



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

Figur 6 Navngiv forbindelsen.

Add Relying Party Trust Wizard ×		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	MODST Prod SSO	
Specify Display Name	Notes:	
 Choose Access Control Policy 		^
Ready to Add Trust		
Finish		
		~

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

Test: MODST Test SSO

Prod: MODST Prod SSO

Figur 7 Sæt adgangskontrol.

输 Add Relying Party Trust Wizard			
Choose Access Contr	ol Policy		
Steps	Choose an access control policy:		
Welcome	Nama	Description	^
Select Data Source		Grant access to even/one	
Specify Display Name	Permit everyone and require MFA	Grant access to everyone and require	e E
Choose Access Control Policy	Permit everyone and require MFA for specific group Permit everyone and require MFA from extranet access	Grant access to everyone and require Grant access to the intranet users an	E
 Ready to Add Trust Finish 	Permit everyone and require MFA from unauthenticated devices Permit everyone and require MFA, allow automatic device registra Permit everyone for intranet access	Grant access to everyone and require Grant access to everyone and require Grant access to the intranet users.	1

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.

Relying Party Trusts				
Display Name	Enabled	Туре	Identifier	Access Control Policy
MODST TEST SSO	Yes	WS-Tr	https://testsso.modst.dk/runtime/	Permit everyone
MODST Prod SSO	Yes	WS-Tr	https://sso.modst.dk/runtime/	Permit everyone

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



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.

Display Name		Enabled	Туре
MODST TEST	Update from Federation Me	tadata	
MODST FIGUE	Edit Access Control Policy		
	Edit Claim Issuance Policy		
	Disable		

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

🙀 Add Transform Claim Rule Wizard				
Select Rule Templa	e e			
Steps	Select the template for the claim rule that you want to create from the following list. The description p			
Choose Rule Type	details about each claim rule template.			
 Configure Claim Rule 	Claim rule template:			
	Send LDAP Attributes as Claims			
	Send LDAP Attributes as Claims			

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



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: <u>https://oes.dk/systemer/faelles-systemer-i-staten/data-og-integrationer/single-sign-on/</u>

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

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from v to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issue from the rule.

Claim rule name:

ldap

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
•	E-Mail-Addresses	https://modst.dk/sso/claims/email
	User-Principal-Name ~	https://modst.dk/sso/claims/userid
	objectGuid ~	https://modst.dk/sso/claims/uniqueid
	Telephone-Number ~	https://modst.dk/sso/claims/mobil
	E-Mail-Addresses	Name

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.



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/adfs/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");
<pre>=> issue(type = "https://modst.dk/sso/claims/logonmethod", value = " username- passwordprotected-transport");</pre>

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

Display Name		Enabled	Туре
MODST TEST	Update from Federation Metao	iata	
MODST FIDE 2	Edit Access Control Policy		
	Edit Claim Issuance Policy		
	Dicablo		

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



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

🙀 Add Transform Claim F	tule Wizard	×		
Select Rule Templat	le			
Steps	Select the template for the claim rule that you want to create from the following list. The description provides			
Choose Rule Type details about each claim rule template.				
Configure Claim Rule	Claim rule template:			
	Send Claims Using a Custom Rule			
	Claim rule template description:			
	Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are	1		

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

You can configue claims from a So issuance statem	ure a custom claim rule, such as a rule that requires multiple incoming claims or that extr L attribute store. To configure a custom rule, type one or more optional conditions and ent using the AD FS claim rule language.	acts an
Claim rule name	:	
CVR		
Rule template:	Send Claims Using a Custom Rule	
Rule template: S Custom rule:	Send Claims Using a Custom Rule	

Listen med regler findes i Tabel 1 LDAP Regler



Figur 15 Nu burde listen over regler se således ud

dit Claim Issuance Policy for MODST TEST SSO			\times	
suance Tr	ansform Rules			
The follow	ving transform rules specify the c	laims that will be sent to the relying party.		
Order	Rule Name	Issued Claims		
1	ldap https://modst.dk/sso/claim			
2 CVR <see claim="" rule=""></see>				
3	Assuancelevel	<see claim="" rule=""></see>		
4	Logonmethod	<see claim="" rule=""></see>		

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.



3 Fejlfinding3.1 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".

	LDAP Attribute (Select or type to add more)		Outgoing Claim Type (Select or type to add more)	
•	E-Mail-Addresses	~	https://modst.dk/sso/claims/email	~
	User-Principal-Name	~	https://modst.dk/sso/claims/userid	~
	objectGuid	~	https://modst.dk/sso/claims/uniqueid	~
	Telephone-Number	~	https://modst.dk/sso/claims/mobil	~
	Display-Name	~	Name	~

CVR	
Rule template: Send Claims Using a Custom Rule	
Custom rule:	
<pre>=> issue(Type = "https://modst.dk/sso/claims/cvr", Va "12345678");</pre>	lue =



4 Claim types hos Statens SSO

Claim	Eksempel værdi	AD Attribute	Beskrivelse
https://modst.dk/sso/claims/email	jodo@myemail.com	E-Mail-	Brugerens E-mail
		Addresses	
https://modst.dk/sso/claims/userid	jodo@myemail.com	User-	Efter aftale med
		Principal-	Økonomistyrelsen kan UPN (User Principal
		Name	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-	Navnet der evt.
		Addresses	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	Institutionens CVRnummer
		AD	



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)