ØKONOMISTYRELSEN

TEKNISK VEJLEDNING

Tilkobling af institution på Statens SSO

2. juni 2025
PAU/finpa

ØKONOMISTYRELSEN

Indholdsfortegnelse

Indledning

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 identity provider over for Statens SSO – dvs. den skal levere validering af brugere. Sidst i denne vejledning er der angivet en tjekliste, som institutionen skal følge ifm. tilkoblingen.

Målgruppen er institutionens teknikere, som arbejder med institutionens Active Directory(AD)/Brugerkatalog.

Det bemærkes, at Statens It står for driften af en stor del af de statslige institutioners Active Directory. Statens It har opgaven med tilkobling til Statens SSO og institutionerne behøver ikke foretage sig yderligere.

Ansvar i forbindelse med Statens SSO

Institutionen skal leve op til Økonomistyrelsens Servicebeskrivelser for Statens SSO, som bl.a. præciserer institutionens ansvar for egene brugere i eget AD og tilgængeligheden af føderationsserveren. Servicebeskrivelsen kan findes på Økonomistyrelsens hjemmeside.

I drift på Statens SSO

Når institutionen er tilkoblet Statens SSO, skal brugerne ikke længere anvende de gamle links til fagsystemerne, hvor der benyttes brugernavn og password.

I stedet skal brugeren anvende de links til fagsystemerne, som giver adgang via Statens SSO. Oversigt over disse links kan findes her: https://oes.dk/systemer/faelles-systemer-i-staten/data-og-integrationer/single-sign-on/

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

Institutionen skal have egen føderationsserver (IdP)

For at blive koblet på Statens SSO kræver det, at institutionen har egen føderationsserver - også kaldet en IdP. Denne IdP vil i det offentlige typisk være et af følgende produkter:

- Microsoft AD FS 2.0, 2.1, 3.0 eller 4.0
- SimpleSamlPhp
- Shibboleth-baseret løsning
- OIOSAML-baseret løsning
- PING identity
- Safewhere Identify

Andre IdP-produkter kan også forekomme, og det er ikke essentielt for tilkoblingen hvilket produkt der anvendes, blot at IdP'en kan anvende SAML 2.0 protokollen, specifikt OIOSAML specifikationen.

Alle ovenstående produkter er i stand til at opfylde denne forudsætning og kan anvendes som pejlemærke, hvis institutionen selv er i tvivl om forholdene.

Institutionen skal kunne udstede SAML 2.0-metadata for deres egen IdP

Institutionen skal udlevere SAML 2.0-baserede metadata til Økonomistyrelsen for at blive koblet på Statens SSO. Disse metadata kan leveres som en url til metadata, hvis de er udstillet på internettet. Hvis de ikke er udstillet på internettet skal institutionen sende metadata som en XML-fil, som skal indlæses på Statens SSO. Denne udveksling sker begge veje, dvs. Økonomistyrelsen modtager metadata fra institutionen, og Økonomistyrelsen udstiller metadata til institutionen.

Økonomistyrelsens metadata er udstillet på internettet og institutionen kan blot referere til metadata url'en jf. nedenfor.

MODST metadata adresser

Følgende webadresser giver adgang til MODST SAML 2.0 metadata for hhv. test- og produktionsmiljøerne i Statens SSO.

Miljø	**Metadata URL**	**Beskrivelse**
Test	https://statens-sso-test.oes.dk/runtime/saml2auth/metadata.idp	Indeholder SAML 2.0 metadata for Statens SSO test
Produktion	https://statens-sso.oes.dk/runtime/saml2auth/metadata.idp	Indeholder SAML 2.0 metadata for Statens SSO produktion

Metadata er sikre at transportere over email og internet

Metadata indeholder ikke persondata eller private sikkerhedsinformationer, og kan af sikkerhedshensyn derfor godt udstilles på internettet. Dette er også normal praksis inden for denne teknologi.

Information vedr. SHA-256 hashing mm.

Statens SSO følger Digitaliseringsstyrelsens anbefaling, og understøtter udelukkende SHA-256 hashing. Institutionen skal understøtte dette, da det er en forudsætning for at kunne tilkoble sig Statens SSO.

Det bemærkes endvidere, at Statens SSO anvender https TLS 1.2 til transport af meddelelser og SHA-256 til signing af meddelelser.

Information om hvilke attributter, institutionen skal medsende fra sin lokale IdP

Statens SSO løsning anvender følgende SAML-attributter for brugerne, som skal være medsendt fra institutionens lokale IdP. Som en hjælp til institutionen, er det endvidere angivet, hvordan institutionen skal mappe disse attributter hvis de bruger Microsofts ADFS. Visse claims specificeres yderligere efter oversigten.

Bemærk, du skal indsætte hele stien, som fremgår i kolonnen Claim type i din opsætning – altså fx ”https://modst.dk/sso/claims/userid”.

Oversigt over attributter

Claim type	**Eksempel på indhold**	**Beskrivelse**	**Mappes fra AD attribut**	**Krævet?**
https://modst.dk/sso/claims/cvr	12349583	Institutionens CVR-nummer	Mappes ikke; medsendes blot i fast claim værdi = institutionens CVR	Ja
https://modst.dk/sso/claims/userid	john@doe.org	Brugerens e-mail (evt. UPN). Efter aftale med Økonomistyrelsen kan UPN (User Principal Name) anvendes. Fagsystemet skal bruge dette claim til at identificere brugeren i fagsystemet.	mail	Ja

Claim type	Eksempel på indhold	Beskrivelse	Mappes fra AD attribut	Krævet?
https://modst.dk/sso/claims/email	john@doe.org	Brugerens e-mail Normalt ligger værdien i AD-attributten ”mail”, men dette er kun vejledende. Hvis institutionen bruger en anden attribut, skal værdien hentes herfra	mail	Ja
https://modst.dk/sso/claims/uniqueid	26307a60-1342-4a4a-9da9-b01c496c4f2d	Indeholder et unikt id for brugeres lokale directory - typisk AD objectGuid. Hvis institutionen ikke bruger Microsoft Windows, skal institutionen aftale med Økonomistyrelsen, hvilken identifikation, der skal medsendes.	objectGuid	Ja

Claim type	Eksempel på indhold	Beskrivelse	Mappes fra AD attribut	Krævet?
https://modst.dk/sso/claims/mobile	004512345678	Brugerens mobiltelefonnummer til SMS til to-faktor-login. Hvis institutionen vælger ikke at medsende denne oplysning, vil institutionens medarbejdere ikke kunne modtage SMS'er ifm. to-faktorlogin. I stedet kan brugeren modtage en e-mail med en to-faktor-kode.	mobile	Valgfri

Claim type	Eksempel på indhold	Beskrivelse	Mappes fra AD attribut	Krævet?
https://modst.dk/sso/claims/assurancelevel	2	Claimet kan have følgende værdier:{2,3 eller højere}. Se specifikation af attributten assurancelevel nedenfor.	Dette claim mappes ikke fra en attribut, men institutionen skal sikre, at det angives, hvordan brugeren er autentificeret.	Ja
https://modst.dk/sso/claims/logonmethod	username-password-protected-transport		Dette claim mappes ikke fra en attribut, men institutionen skal sikre, at det angives, hvordan brugeren er logget på.	Ja
https://modst.dk/sso/claims/surname	Jensen	Brugerens efternavn	sn	Nej
https://modst.dk/sso/claims/givenname	John	Brugerens fornavn	givenname	Nej
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	john@doe.org	Samme værdi, som indsat i https://modst.dk/sso/claims/userid	Mail	Ja

Specifikation af attributten assurancelevel

Attributten assurancelevel fortæller, hvor stærkt brugeren er autentificeret af den lokale IdP. Oplysningen vil blive brugt af Statens SSO sammen med loginmetoden til at afgøre, om Statens SSO skal afkræve to-faktor-login via Statens SSO, hvis brugeren er for svagt autentificeret.

Oplysningen skal jf. oversigten nedenfor ligge i denne attribut:
https://modst.dk/sso/claims/assurancelevel

Økonomistyrelsen kræver, at assurancelevel er mindst niveau 2 (enkeltfaktor login), hvorfor værdier på 2 eller højere (to-faktor eller lignende) er accepteret.

Attributten kan antage værdierne 2, 3 eller højere. Nedenfor er det specificeret, hvornår en værdi skal bruges.

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.
Højere værdier	Højere værdier bruges pt. ikke og vil blive behandlet som værdien 3.

Specifikation af attributten logonmethod

Attributten logonmethod beskriver hvilken loginmetode, brugeren har anvendt ved login på den lokale IdP. Oplysningen bliver brugt sammen med assurancelevel attributten, til at vurdere om brugeren skal præsenteres for to-faktor login på Statens SSO.

Oplysningen skal jf. oversigten ligge i denne attribut:
https://modst.dk/sso/claims/logonmethod

Nedenfor er de værdier specificeret, som Attributten kan antage.

Specifikation af værdier i logonmethod

Værdi	Beskrivelse
username-password-protected-transport	Brugeren er logget på via eksplicit indtastning af brugernavn/adgangskode via SSL transport – f.eks. formsbaseret AD FS login.
kerberos-spnego	Brugeren er logget på via sit lokale domæne og login'et på sin arbejds PC.
two-factor	Brugeren er logget på via en form for to-faktor. Det kan være feks. enkelt faktor + sms kode eller nemid.

Oplysninger om domæner

Institutionen skal oplyse Økonomistyrelsen om, hvilke domæner og subdomæner, som indgår i institutionens e-mails, dvs. de oplysninger, der fremgår efter snabel-a'et - @ - i institutionens e-mailadresser.

Statens SSO anvender dette til at sikre, at brugeren kommer fra den rigtige institution.

Test af forbindelse til Statens SSO

Institutionen kan selv teste, om der er forbindelse til Statens SSO på en af nedenstående url'er (hhv. test og produktion).

Miljø	**Url**
Test	https://statens-sso-test.oes.dk/samlclaimapp1/
Produktion	https://statens-sso.oes.dk/samlclaimapp1/

Institutionenen skal dog manuelt kontrollere, om det er de rigtige oplysninger, der er lagt i claims'ene.

Tjekliste ifm. tilslutning til Statens SSO

Nedenfor er en oversigt over de aktiviteter, der skal gennemføres ifm. tilslutning af en institution til Økonomistyrelsens single sign-on-løsning (Statens SSO).

Nr.	Aktivitet	Ansvarlig	Gennemført (til institutionens opfølgning)
1	**OPSTART**		
1.1	Opsætning af institutionens føderationsserver (fx AD FS)	Institutionen	
1.2	Institutionen oplyser følgende oplysninger via serviceportalen: • Metadataurl('er) for institutionens føderationsserver. • Domæne og evt. subdomæner for institutionens e-mail-adresser. • Institutionens kontaktpersoner og kontaktoplysninger. Serviceportalen: https://serviceportal.statens-adm.dk/ Hvis institutionen har et test-AD, skal institutionen både oplyse metadata-URL for test-AD og for produktionsAD'et.	Institutionen	
1.3	Økonomistyrelsen sender vejledning med metadataurl for Statens SSO (produktion og test) til institutionens kontaktperson.	Økonomistyrelsen	
2	**TESTMILJØ**		
2.1	Institutionen konfigurerer sin føderationsserver med metadataurl'en for Statens SSO (hhv. produktion og test) og konfigurerer de relevante SAML-attributter jf. vejledning.	Institutionen	
2.2	Økonomistyrelsen konfigurerer Statens SSO-test med metadataurl'en for institutionen.	Økonomistyrelsen	
2.3	Institutionen tester forbindelsen til Statens SSO-test ved at klikke på dette link: https://statens-sso-test.oes.dk/samlclaimapp1/MyPage.aspx	Institutionen	
2.4	Evt. fejlfinding	Økonomistyrelsen og institutionen	
3	**PRODUKTIONSMILJØ**		

Nr.	Aktivitet	Ansvarlig	Gennemført (til institutionens opfølgning)
3.1	Økonomistyrelsen konfigurerer Statens SSO-produktion med metadataurl'en for institutionen.	Økonomistyrelsen	
3.2	Institutionen kontrollerer forbindelsen til Statens SSO-produktion ved at klikke på https://statens-sso.oes.dk/samlclaimapp1/MyPage.aspx Institutionen klikker på det link i fagsystemet, der giver adgang til fagsystemet via Statens SSO.	Institutionen	
3.3	Evt. fejlfinding	Økonomistyrelsen og institutionen	
3.4	Institutionen bekræfter tilslutningsaftalen, som Økonomistyrelsen fremsender	Institutionen	
3.5	Når institutionens brugere har direkte adgang til de relevante fagsystemer uden at skulle angive password til fagsystemet, er institutionen i drift via Statens SSO.	n/a	