ØKONOMISTYRELSEN

TEKNISK VEJLEDNING

Tilkobling af fagsystem på Statens SSO

10. september 2020

ØKONOMISTYRELSEN

Indholdsfortegnelse

Indledning

Dette dokument beskriver, hvad man skal gøre for at koble et fagsystem single sign-on-løsningen til de fællesstatslige systemer (SSO-løsningen). Fagsystemet har i dette tilfælde rollen service provider overfor SSO-løsningen – dvs. den skal levere adgangen til den funktionalitet, som fagsystemet indeholder.

Fagsystemet skal have egen føderationsserver (SP)

For at blive koblet på SSO-løsningen kræver det at fagsystemet har egen føderationsserver - også kaldet en SP (Service provider). Denne SP 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 SP-produkter kan også forekomme, og det er ikke essentielt for tilkoblingen hvilket produkt der anvendes, blot at SP'en kan anvende SAML 2.0 protokollen, specifikt OIOSAML specifikationen jf. https://www.digitaliser.dk/group/42063/resources.

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

Fagsystemet skal kunne udstede SAML 2.0-metadata for deres egen SP

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

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

Økonomistyrelsen metadata adresser

Følgende webadresser giver adgang til Økonomistyrelsen SAML 2.0 metadata for hhv. test- og produktionsmiljøerne hos Økonomistyrelsen.

Miljø	Metadata URL	Beskrivelse
Test	https://testsso.modst.dk/runtime/saml2/metadata.idp	Indeholder SAML 2.0 metadata for Økonomistyrelsen test
Produktion	https://sso.modst.dk/runtime/saml2/metadata.idp	Indeholder SAML 2.0 metadata for Økonomistyrelsen produktion

Metadata er sikre at transportere over e-mail og internet

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

Information vedr. SHA-256 hashing mm.

SSO-løsningen følger Digitaliseringsstyrelsens anbefaling, og understøtter udelukkende SHA-256 hashing, se evt. https://www.digitaliser.dk/news/3554079. Fagsystemet skal understøtte dette, da det er en forudsætning for at kunne tilkoble sig SSO-løsningen.

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

SSO-løsningen på oes.dk

Du kan læse mere om SSO-løsningen her:

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

Information om hvilke attributter der kan sendes til fagsystemet

SSO-løsningen løsning anvender nedenstående SAML-attributter. Disse attributter er dem, der er mulige for SSO-løsningen at præsentere over for det pågældende fagsystem.

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 Visse institutioner sender dog pt. ikke CVR-nr.
https://modst.dk/sso/claims/userid	john@doe.org	Brugerens e-mail (evt. UPN). Efter aftale med Moderniseringsstyrelsen kan UPN (User Principal Name) anvendes. Fagsystemet skal bruge dette claim til at identificere brugeren i fagsystemet.	mail	Ja
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

Claim type	Eksempel på indhold	Beskrivelse	Mappes fra AD attribut	Krævet?
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 Moderniseringsstyrelsen, hvilken identifikation, der skal medsendes.	objectGuid	Ja
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
https://modst.dk/sso/claims/assurancelevel	2	Claimet kan have følgende værdier:{2,3 eller højere}	Dette claim mappes ikke fra en attribut, men institutionen skal sikre, at det angives, hvordan brugeren er autentificeret.	Ja

Claim type	Eksempel på indhold	Beskrivelse	Mappes fra AD attribut	Krævet?
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