ØKONOMISTYRELSEN

Tilslutning af fagsystem på Statens SSO

Indhold

Indledning

Dette dokument beskriver, hvordan et fagsystem tilsluttes den fællesstatslige Single Sign-On-løsning (Statens SSO).

I denne sammenhæng fungerer fagsystemet som Service Provider (SP) over for SSO-løsningen og stiller den funktionalitet, som fagsystemet indeholder, til rådighed for autentificerede brugere.

Tekniske forudsætninger for tilkobling til Statens SSO

Krav om føderationskomponent i fagsystemet (Service Provider)

For at kunne tilkoble Statens SSO skal fagsystemet have en føderationskomponent, der fungerer som Service Provider (SP). SP'en anvendes til at modtage og validere autentificeringsoplysninger fra Statens SSO.

I den offentlige sektor anvendes typisk én af følgende SP-løsninger:

- Microsoft AD FS (version 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 anvendes. Det er ikke afgørende for tilkoblingen, hvilket produkt der vælges, så længe SP'en understøtter SAML 2.0-protokollen, herunder OIOSAML-specifikationen, jf. Digitaliseringsstyrelsens standarder: https://digst.dk/it-loesninger/standarder/oiosaml-profiler/

De nævnte produkter opfylder alle dette krav og kan anvendes som pejlemærke, hvis fagsystemets teknikere er i tvivl om valg af løsning.

Krav om udstedelse af SAML 2.0-metadata

For at fagsystemet kan blive tilkoblet Statens SSO, skal fagsystemets teknikere udlevere SAML 2.0-baserede metadata for fagsystemets SP til Økonomistyrelsen.

Metadataudvekslingen sker gensidigt, idet Økonomistyrelsen både modtager metadata fra fagsystemet og stiller egne SAML 2.0-metadata til rådighed for fagsystemet.

Metadata kan leveres på én af følgende måder:

- Som en URL til metadata, hvis metadata er udstillet på internettet
- Som en XML-fil, hvis metadata ikke er offentligt tilgængelige

Hvis metadata leveres som en URL, overvåger Statens SSO løbende denne URL og opdaterer automatisk sine oplysninger, når institutionen ændrer i metadata. Dette er den foretrukne metode, da den sikrer, at Statens SSO altid har opdaterede oplysninger uden manuel indgriben.

Uanset format kan metadata fremsendes til Økonomistyrelsen via Serviceportalen hos Statens Administration, hvor der vælges kategorien Øvrige og herefter SSO.

Økonomistyrelsens metadata-URL'er

For at konfigurere SP'en korrekt skal institutionen anvende Økonomistyrelsens SAML 2.0-metadata. Metadata er tilgængelige for henholdsvis test- og produktionsmiljøerne i Statens SSO via følgende URL'er:

Miljø	Metadata url	Beskrivelse
Test:	https://statens-sso-test.oes.dk/runtime/saml2/metadata.idp	Indeholder SAML 2.0 metadata for Statens SSO test
Prod:	https://statens-sso.oes.dk/runtime/saml2/metadata.idp	Indeholder SAML 2.0 metadata for Statens SSO produktion

Metadata kan transporteres sikkert via e-mail og internet

Metadata indeholder hverken persondata eller følsomme sikkerhedsoplysninger og kan derfor transporteres eller udstilles på internettet uden sikkerhedsrisiko. Dette er almindelig praksis inden for SAML 2.0-teknologi og føderationsløsninger.

Kryptering og signering

Statens SSO følger Digitaliseringsstyrelsens anbefalinger og understøtter udelukkende SHA-256 hashing. Institutionens IdP skal også understøtte SHA-256, da det er en forudsætning for tilkobling til Statens SSO.

Derudover anvender Statens SSO HTTPS (TLS 1.2) til transport af meddelelser og SHA-256 til signering af meddelelser, hvilket sikrer både integritet og sikkerhed i kommunikationen.

Krav til SAML-attributter til fagsystemet (service provider)

Statens SSO kan præsentere nedenstående SAML-attributter (claims) for fagsystemet som led i autentificeringen. Tabellen viser de attributter, som er tilgængelige fra Statens SSO, og som fagsystemet skal anvende i sin konfiguration.

Claim navn	Eksempelværdi	Formål/ beskrivelse	Kildeattribut i AD
https://modst.dk/sso/claims/cvr	12349583	Institutionens CVR-nummer. Medsendes som fast claimværdi.	-
https://modst.dk/sso/claims/userid	john@doe.org	Brugerens unikke ID (typisk e-mail). UPN kan anvendes efter aftale med Økonomistyrelsen.* Fagsystemerne bruger dette claim til at identificere brugeren.	Mail
https://modst.dk/sso/claims/uniqueid	26307a60-1342-4a4a-9da9-b01c496c4f2d	Indeholder et unikt ID for brugeren i det lokale directory (typisk AD objectGuid). Hvis institutionen ikke bruger	objectGuid
https://modst.dk/sso/claims/assurancelevel	3	Angiver brugerens autentificeringsniveau. Kan have værdien 3, da Økonomistyrelsen kræver at brugerne kommer fra et sikret netværk Mappes ikke fra AD; institutionen skal sikre korrekt angivelse af autentificeringsniveau.	-
https://modst.dk/sso/claims/logonmethod	Usernamepassword protectedtransport	Dette claim mappes ikke fra en attribut, men institutionen skal	-

		sikre, at det angives, hvordan brugeren er logget på.	
http://sche-mas.xmlsoap.org/ws/2005/05/iden-tity/claims/name	john@doe.org	Brugerens e-mail	Mail