ØKONOMISTYRELSEN

Statens SSO med Microsoft Active Directory Federation Services (ADFS)

Indhold

Indledning

Dette dokument beskriver de krav og handlinger, en institution skal opfylde for at blive tilkoblet Økonomistyrelsens single sign-on-løsning (Statens SSO). Institutionen fungerer i denne sammenhæng som *identity provider* over for Statens SSO og har dermed ansvaret for at validere brugere.

Vejledningen afsluttes med en tjekliste, som institutionen skal følge i forbindelse med tilkoblingen.

Målgruppen for dokumentet er institutionens tekniske medarbejdere med ansvar for institutionens Active Directory (AD) eller brugerkatalog.

Det bemærkes, at Statens It varetager driften af Active Directory for en stor del af de statslige institutioner. For disse institutioner håndterer Statens It tilkoblingen til Statens SSO, og der kræves derfor ingen yderligere handling fra institutionernes side.

Institutionens forpligtelser i relation til Statens SSO

Institutionen er ansvarlig for at efterleve Økonomistyrelsens servicebeskrivelser for Statens SSO, herunder ansvaret for administration af egne brugere i institutionens Active Directory (AD) samt for drift og tilgængelighed af føderationsserveren. Servicebeskrivelsen er tilgængelige på Økonomistyrelsens hjemmeside: https://oes.dk/digitale-loesninger/om-statens-digitale-loesninger/servicebeskrivelser/

Adgang til fagsystemer efter tilkobling til Statens SSO

Når institutionen er tilkoblet Statens SSO, skal brugerne ikke længere anvende de tidligere links til fagsystemerne, hvor login sker med brugernavn og adgangskode.

I stedet skal brugerne benytte de links til fagsystemerne, som giver adgang via Statens SSO. En oversigt over disse links findes på Økonomistyrelsens hjemmeside: https://oes.dk/digitale-loesninger/statens-single-sign-on/systemer-tilsluttet-statens-sso/

Det bemærkes, at enkelte fagsystemer desuden tilbyder adgang via Statens SSO direkte fra systemets normale login-side, typisk via en særskilt single sign-on-knap.

Tekniske forudsætninger for tilkobling til Statens SSO

Krav om egen føderationsserver (IdP)

For at blive tilkoblet Statens SSO skal institutionen have sin egen føderationsserver (identity provider, IdP). IdP'en anvendes til autentifikation af institutionens brugere over for Statens SSO.

I den offentlige sektor anvendes typisk én af følgende IdP-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 IdP-produkter kan også anvendes. Det er ikke afgørende for tilkoblingen, hvilket produkt der vælges, så længe IdP'en understøtter SAML 2.0-protokollen og specifikt OIOSAML-specifikationen.

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

Krav om udstedelse af SAML 2.0-metadata

Institutionen skal udlevere SAML 2.0-baserede metadata for sin IdP til Økonomistyrelsen for at blive tilkoblet Statens SSO.

Metadataudvekslingen sker gensidigt: Økonomistyrelsen modtager metadata fra institutionen og stiller egne SAML 2.0-metadata til rådighed for institutionen.

Metadata kan leveres på to måder:

- Som en URL til metadata, hvis metadata er offentligt tilgængelige 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 foretager ændringer 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 institutionens IdP 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/saml2auth/metadata.idp	Indeholder SAML 2.0 metadata for Statens SSO test
Prod:	https://statens-sso.oes.dk/runtime/saml2auth/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.

Domæner for e-mailadresser

Institutionen skal oplyse Økonomistyrelsen om de domæner og subdomæner, som anvendes i institutionens e-mailadresser – altså den del, der følger efter @ i adressen.

Statens SSO bruger disse oplysninger til at verificere, at brugeren tilhører den korrekte institution.

Krav til SAML-attributter fra institutionens IdP

For at Statens SSO kan fungere korrekt, skal institutionens IdP medsende følgende SAML-attributter for brugerne.

Som hjælp til opsætning er der i tabellen nedenfor angivet, hvordan attributterne kan mappes, hvis institutionen anvender Microsoft ADFS. Det er vigtigt, at alle påkrævede attributter leveres korrekt, da manglende eller forkert opsatte attributter kan forhindre korrekt login via Statens SSO.

Bemærk: Når du opsætter claims, skal hele navnet fra kolonnen Claim navn indsættes i IdP'en, fx: https://modst.dk/sso/claims/userid

Oversigt over attributter

Bemærk: Visse claims kan have yderligere specifikationer, som uddybes yderligere i det efterfølgende afsnit.

Påkrævede claims/attributter			
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/email	john@doe.org	Brugerens e-mailadresse. Normalt fra AD-attributten mail, men en anden AD-attribut kan anvendes, hvis relevant.	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 Microsoft Windows, skal værdien aftales med Økonomistyrelsen.	objectGuid

Tabel fortsættes på næste side - - - >

Påkrævede claims/attributter			
Claim navn	**Eksempelværdi**	**Formål/ beskrivelse**	**Kildeattribut i AD**
https://modst.dk/sso/claims/assurancelevel	2	Angiver brugerens autentificeringsniveau. Kan have værdier 2, 3 eller højere. 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://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	john@doe.org	Samme værdi, som indsat i https://modst.dk/sso/claims/userid	Mail
Valgfrie claims/attributter			
https://modst.dk/sso/claims/mobile	004512345 678	Brugerens mobiltelefonnummer til SMS ved tofaktor-login. Hvis ikke medsendt, kan brugeren i stedet modtage tofaktor-kode via e-mail.	mobile
https://modst.dk/sso/claims/surname		Efternavn på brugeren	sn
https://modst.dk/sso/claims/givenname		Fornavn på brugeren	givenname

Yderligere specifikationer

Assurancelevel

Attributten assurancelevel (https://modst.dk/sso/claims/assurancelevel) angiver, hvor stærkt brugeren er autentificeret af den lokale IdP. Statens SSO anvender denne information sammen med loginmetoden til at afgøre, om der skal kræves to-faktor-login, hvis brugeren er for svagt autentificeret.

Økonomistyrelsen kræver minimum niveau 2 (enkeltfaktor-login). Værdier på 2 eller højere (fx to-faktor) er accepteret.

Attributten kan antage værdierne 2 eller 3, afhængigt af brugerens autentificeringsstyrke.

Nedenfor specificeres, hvornår hver værdi skal anvendes:

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.

Logonmethod

Attributten logonmethod (https://modst.dk/sso/claims/logonmethod) angiver, hvilken loginmetode brugeren har anvendt ved autentificering på den lokale IdP. Statens SSO bruger denne information sammen med assurancelevel til at afgøre, om brugeren skal præsenteres for to-faktor-login.

Nedenfor er de tilladte værdier for attributten specificeret:

Værdi	Beskrivelse
username-password-protectedtransport	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.

Test af tilkobling til Statens SSO

Institutionen kan selv teste forbindelsen til Statens SSO ved at anvende en af følgende URL'er:

- Testmiljø: https://statens-sso-test.oes.dk/samlclaimapp1/MyPage.aspx
- Produktionsmiljø: https://statens-sso.oes.dk/samlclaimapp1/MyPage.aspx

Bemærk: Institutionen skal manuelt kontrollere, at de korrekte oplysninger er inkluderet i alle claims.

Tjekliste for tilslutning til Statens SSO

Nr.	Aktivitet	Ansvarlig
1	Opsætning af institutionens føderationsserver (fx AD FS)	Institutionen
2	Institutionen oplyser følgende oplysninger via serviceportalen, hos Statens Administration, hvor der vælges kategorien Øvrige og herefter SSO: • Metadataurl('er) for institutionens føderationsserver. • Domæne og evt. subdomæner for institutionens e-mail-adresser. • Institutionens kontaktpersoner og kontaktoplysninger. Link til 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
3	Institutionen konfigurerer sin føderationsserver med metadataurl'en for Statens SSO (hhv. produktion og test) og konfigurerer de relevante SAML-attributter jf. vejledningen, afsnit Økonomistyrelsens metadata-URL'er og Krav til SAML-attributter fra institutionens IdP	Institutionen
4	Økonomistyrelsen konfigurerer Statens SSO-test med metadataurl'en for institutionen.	Økonomistyrelsen
5	Institutionen tester forbindelsen til Statens SSO-test ved at klikke på nedenstående link: https://statens-sso-test.oes.dk/samlclaimapp1/MyPage.aspx	Institutionen
6	Evt. Fejlfinding	Institutionen og Økonomistyrelsen
7	Økonomistyrelsen konfigurerer Statens SSO-produktion med metadataurl'en for institutionen.	Økonomistyrelsen
8	Institutionen kontrollerer forbindelsen til Statens SSO-produktion ved at klikke på nedenstående link: https://statens-sso.oes.dk/samlclaimapp1/MyPage.aspx Institutionen logger på et vilkårligt fagsystem via SSO.	Institutionen
9	Evt. Fejlfinding Når institutionens brugere har direkte adgang til de relevante fagsystemer uden at skulle angive password til fagsystemet, er institutionen i drift via Statens SSO.	Institutionen og Økonomistyrelsen