

How-To - Ställa krav på inloggning via SWAMID vid upphandling

Vid upphandling av system kan en organisation vilja ställa krav på att SWAMID ska användas vid inloggning. Nedan finns ett exempel på hur detta kan se ut.

Upphandlingskrav på SWAMID-inloggning

Systemet ska stödja inloggning via identitetsfederation baserat på SAML 2.0 Web Browser SSO Profile enligt SAML V2.0 Deployment Profile for Federation Interoperability [SAML2int]. Särskild hänsyn ska tas till avsnitt 2.2.1 i SAML2int. Metadata ska automatiskt hämtas och uppdateras via antingen SAML Profile for the Metadata Query Protocol [SAML-MDQ] eller publicerat metadata aggregat med mer än en identitetsutgivare (IdP) enligt avsnitt 2.3.1 i Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0 [SAML2Meta].

E-postadress som användaridentIFIERARE är kraftigt olämpligt med avseende på att en e-postadress är inte långsiktigt unik utan kan senare kopplas till en annan person. Att använda e-postadressen som identifierare kan leda till att data såsom personuppgifter kan komma i orätta händer och därför rekommenderas i stället att en annan identifierare används. Inom identitetsfederationer används en långsiktigt unik identifierare, som ser ut som en e-postadress men inte är det, för att uppnå långsiktig unikhet. Exempel på dessa identifierare är samlPairwiseID (urn:oasis:names:tc:SAML:attribute:pairwise-id) och samlSubjectID (urn:oasis:names:tc:SAML:attribute:subject-id) [SAMLSubId] samt den äldre eduPersonPrincipalName (urn:oid:1.3.6.1.4.1.5923.1.1.1.6) [eduPerson].

Referenser:

- eduPerson - eduPerson and eduOrg Object Classes, <https://refeds.org/specifications/eduperson>
- SAML2int - SAML V2.0 Deployment Profile for Federation Interoperability, <https://kantarainitiative.github.io/SAMLprofiles/saml2int.html>
- SAML-MDQ - SAML Profile for the Metadata Query Protocol, <https://www.ietf.org/id/draft-young-md-query-saml-18.html>
- SAML2Meta - Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>
- SAMLSubId - SAML V2.0 Subject Identifier Attributes Profile Version 1.0, <https://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.pdf>