Allmänna riktlinjer

Allmänna riktlinjer

SWAMID SAML WebSSO är baserad på användning av signerad SAML2 metadata. Federationen stödjer både SAML1.1 (shibboleth-profilen) och SAML2-entiteter men SAML2 är den rekommenderade teknologin.

Federationspolicyn innehåller inga formella krav på tekniska profiler. All syntaktiskt korrekt metadata kan registreras och publiceras men för att uppnå interoperabilitet med andra entiteter (SP:er och IdP:er) så gäller följade tekniska rekommendationer:

SAML-Profiler

Följande SAML-profiler (per SAML-version) är rekommenderade. Notera att Shibboleth-profilen av SAML 1.1 är baserad på användning av SAML2 metadata.

SAML1.1	Shibboleth SAML 1.1
SAML2	Interoperable SAML 2.0 Profile

Implementationer

Följande produkter/implementationer av SAML är väl testade och fungerar väl med SWAMID SAML WebSSO:

- Shibboleth
- simpleSAMLphp

Följande produkter/implementationer av SAML är delvis testade eller otestade men vi har anledning att tro att de fungerar med SWAMID SAML WebSSO:

- Microsoft Geneva
- NordicEdge Identity Manager

Metadata

Metadata som publiceras följer SAML V2.0 Metadata Interoperability Profile Version 1.0.

Certifikat

SWAMID SAML WebSSO använder certifikat i metadata för att binda nycklar till SAML-entiteter till skillnad från vissa federationer som använder en PKI som utfärdar certifikat för entiteterna i federationen. Federationen har inga synpunkter på hur dessa certifikat skapats. Både självsignerade eller certifikat utfärdade av en CA accepteras i metadata.

Kontaktinformation i metadata

Kontaktinformation i metadata bör bestå av minst en epost-address per entitet. För IdP:er krävs minst en technical contact med fullständigt namn samt epost-address.

SAML Extensioner

Alla IdP:er måste stödja Shibboleth 'Scope'. Scope måste vara samma som någon domän som ägs av den organisation som ansvarar för IdP:n.

Attribut-behov (attribute requirements)

Alla SP:er bör inkludera sk attribute requirements in SAML-metadata genom att inkludera ett eller flera <RequestedAttribute>-element i en <AttributeConsumingService>. Dessa element parsas av sk consent-funktioner i IdP:er som ger användare möjlighet att acceptera (eller inte) att attribut skickas från IdP:n till SP:n.