SWAMID

Swedish Academic Identity Federation

SWAMID SAML WebSSO Technology Profile

Presentation och diskussion om ny version

2021-11-09

SWAMID

Community Consensus Process
SWAMID SAML WebSSO Technology Profile

- Vid varje förändring av SWAMID:s policyramverk ska förändringen förankras inom SWAMID genom en konsultationsprocess
- Förändringen får inte beslutas av SWAMID Board of Trustees utan att konsultationsprocess har genomgåtts
- 25 oktober – Operations skickar ut teknologiprofilen
- 9 november – Konsultationsmöte
- 19 november – Sista dagen för kommentarer
- Diskutera och kommentera idag samt på saml-admins

SWAMID

Varför en uppdaterad profil?

- Nuvarande SAML-profil hänvisade endast till profilen saml2int
- Omvärldskraven på SWAMID som federation har ändrats
  - 2018 – eduGAIN SAML profile beslutades
  - 2019 – Ny version av SAML V2.0 Deployment Profile for Federation Interoperability (saml2int)
  - Utökad användning av SAML-element beroende på krav från olika håll, t.ex. användbarhet (MDUI), entitetskategorier, tillitssignalering och autentiseringskrav
  - Begränsningar i vissa SAML-implementationer (primärt ADFS)
- Samordna med övriga delar i SWAMIDs policyramverk

Kort om förslaget

- Teknologiprofilen är väldigt omfattande (23 sidor)
  - Uppdelad på identitetsutfärdare, tjänster och federationsoperatören
- I princip alla krav som finns på identitetsutfärdare och tjänster har redan tidigare funnits beroende på interoperabilitetskrav men nu blir det tydligt och mätbart
  - Krav vid interfederation
  - Praktiska krav vid användning av olika federationsprogramvaror
- Så få externa krav som möjligt (med några få undantag)

Läsguide

- Identity Provider
  - Compliance and Audit, sida 3
  - Organisational Requirements, sida 3
  - Operational Requirements, sida 5—14
- Relying Party (Service Provider)
  - Compliance and Audit, sida 3
  - Organisational Requirements, sida 4
  - Operational Requirements, sida 14—21
- Federation Operator
  - Organisational Requirements, sida 4—5
  - Operational Requirements, sida 21—23

SWAMID

Compliance and Audit

- Registrerade entiteter måste minst var tolfte månad verifiera och meddela SWAMID att teknologiprofilen fortfarande uppfylls
- Nya metadataverktyget på https://metadata.swamid.se validerar metadata och URL:er som kan valideras med automatik
  - Valideringsfel (error) när krav med MUST (NOT) inte uppfylls
  - Valideringsvarningar (warning) när krav med SHOULD (NOT) eller RECOMMENDED inte uppfylls
- Identitetsutfärdare validerar attributrelease och multifaktor-inloggning via https://release-check.swamid.se
- Det som inte går att validera med automatik hanteras via egenkontroll

Organisational Requirements

- Formella kriterier för att få registreras i SWAMID:
  - Identitetsutfärdare (IdP) måste vara medlemmar samt uppfylla minst en tillitsprofil (SWAMID AL1/AL2/AL3)
  - Tjänster (RP) måste förutom att acceptera SWAMID Metadata Terms of Access and Use vara en tjänst som antingen
    - ägs av en medlem,
    - har en aktiv överenskommelse med och används av minst en medlem,
    - ägs av en myndighet och används av minst en medlem,
    - (åtminstone till del) används för att stödja forskning och utbildning, eller
    - har ett särskilt godkännande av SWAMID Board of Trustees

Organisational Requirements

- Krav på att IdP och RP som inte längre används avregistreras av ägaren
- Krav på att IdP, RP och federationsoperatör följer SWAMID Incident Management Procedure vid misstänkt säkerhets-incident
- Federationsoperatören är skyldig att verifiera att vissa krav i teknologiprofilen uppfylls vid godkännande av registrering och uppdatering av metadata

Operational Requirements

- De operationella kraven skiljer sig mellan IdP och RP men det grundläggande är lika
- Vi kommer endast visa exempel på de operationella kraven i denna presentation
- Avbryt och fråga om ni har frågor inom de olika områdena när vi flyger över dem

Operational Requirements
Metadata registration

- Krav på metadataelement som är till för att underlätta för användare
  - Metadata Extensions for Login and Discovery User Interface (MDUI)
  - Organisationsinformation
  - Felhantering via errorURL
- Krav på metadataelement för entitetskategorier, tillitsprofiler och attribut
- Krav på kontaktinformation, säkerhetskontakt rekommenderas och ska anges om inte särskilda skäl föreligger

Operational Requirements
SAML Keys and Certificates

- Krav på SAML-certifikat för befintliga entiteter (fram till 2030)
  - Minst 2048 bitars nyckellängd för signerings- och krypteringsnycklar då RSA/DSA används
  - Minst 256 bitars nyckellängd för signerings- och krypteringsnycklar då ECC (eliptiska kurvor) används
- Krav på SAML-certifikat för nya entiteter samt vid nyckelrullning
  - Minst 4096 bitars nyckellängd för signerings- och krypteringsnycklar då RSA/DSA används
  - Minst 384 bitars nyckellängd för signerings- och krypteringsnycklar då ECC används

Operational Requirements
SAML Keys and Certificates

- Krav på att SAML-certifikaten är giltiga
  - Inte ett krav i SAML utan beroende på interoperabilitet
  - ADFS måste ha giltiga certifikat
  - 10-årig livslängd rekommenderas i vägledande kommentarer
- Om inte särskilda skäl föreligger ska SAML-certifikaten vara självsignerade
- Krav på att svaga eller komprometterade SAML-certifikat byts
- Krav på att kunna hantera nyckelrullning genom multipla SAML-certifikat

Operational Requirements
Endpoint security

- Krav på att entiteter inte får använda SSL/TLS-protokoll som inte längre anses säkra (deprecated)
  - För närvarande är endast TLS v1.2 och nyare tillåtna
  - Detta är ett av de få externa beroendena i teknologiprofilen
- Krav på att aktuella sårbarheter i webbprotokollen hanteras

Operational Requirements
Software requirements

- Krav på nedladdning och validering av metadata
  - Hur ofta det ska laddas och att signatur ska valideras
- Krav på att IdP ska ha stöd för signalering av inloggningsmetoder (MFA) och forcerad inloggning (ForceAuthn) och hur RP använder detta
- Krav på hur stor klockdrift som tillåts
- Krav på att IdP och RP inte får använda federativ programvara som inte längre uppdateras eller har kända säkerhetshål
  - Detta gäller även äldre versioner av programvara

Operational Requirements
Attribute Release

- Inga formella krav på att en IdP måste genomföra attributrelease men däremot hur det görs
- Krav på vilka användaridentifierare en IdP ska stödja
- Rekommendationer för användning av entitetskategorier
- Krav på användningen av domänbegränsade attribut (scoped)
- Krav på att attributvärden måste uppdateras inom en vecka efter att de ändrats genom organisationens administrativa processer
- Krav och rekommendationer för signalering av tillit

Operational Requirements
Federation Operator

- Metadata management
  - Innehåller krav på vilken information som ska finnas i början av varje signerad metadata
  - Innehåller krav på vilken information som ska finnas i början av varje entitet som publiceras i signerad metadata
- SAML Federation Metadata signing
  - Innehåller krav på hur metadata ska signeras inkl. nyckellängder och hashalgoritmer
- Metadata publishing
  - Innehåller krav på hur metadata ska publiceras

SWAMID

Frågor, kommentarer och diskussion...

SWAMID

SWAMID

Swedish Academic Identity Federation