INTERNET STIFTELSEN

Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkar för ett internet som bidrar positivt till människan och samhället.

INTERNET STIFTELSEN

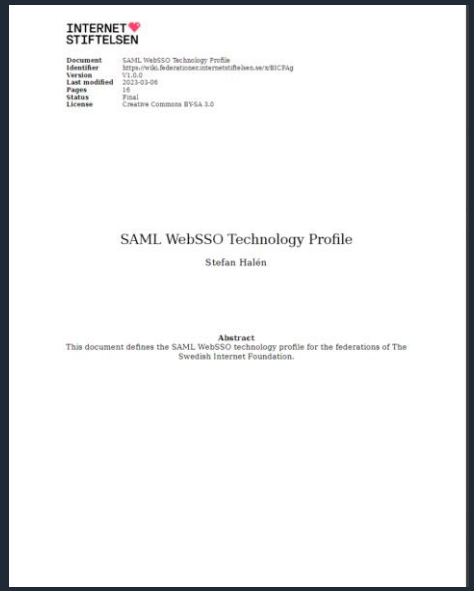
Hur påverkar den nya tekniska profilen den framtida utvecklingen i federationen

Stefan Halén, Internetstiftelsen

Rasmus Larsson, Internetstiftelsen

SAML WebSSO Technical Profile

- 8 mars lanserades SAML WebSSO Technical Profile för Skolfederation
- Profilen är generell och kommer framöver implementeras även för Sambi
- Profilen är en del av federationens policy och måste följas av alla tekniskt anslutna medlemmar i Skolfederation
- Den tekniska efterlevnaden är däremot än inte påtvingad i Federationsadmin (exempelvis med regler i metadatavalidatortjänsten)
- Vi vill ge en bakgrund och vad profilen innebär för federationens medlemmar


INTERNET STIFTELSEN

Document	SAML WebSSO Technology Profile
Identifier	https://wiki.federationer.internetstiftelsen.se/x/BICPAg
Version	V1.0.0
Last modified	2023-03-06
Pages	16
Status	Final
License	Creative Commons BY-SA 3.0

SAML WebSSO Technology Profile

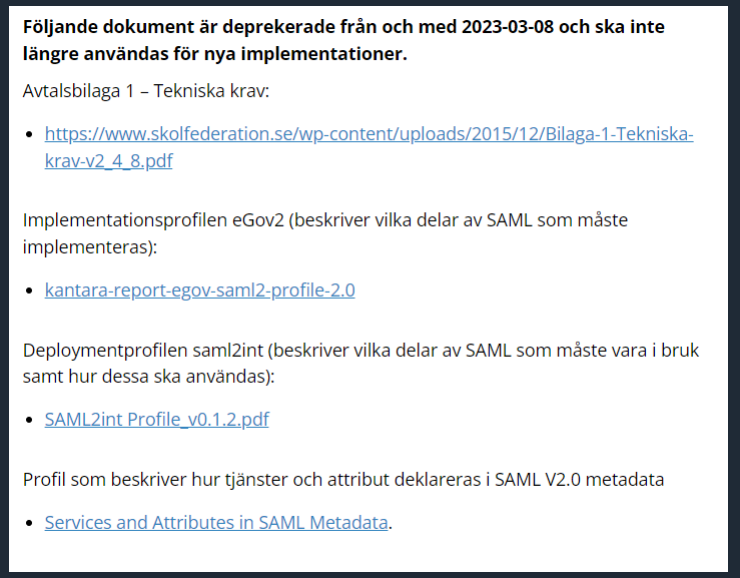
Stefan Halén

Abstract

This document defines the SAML WebSSO technology profile for the federations of The Swedish Internet Foundation.

SAML WebSSO Technical Profile

- Den nya tekniska profilen ersätter tidigare avtalsbilaga och profiler:
  - Avtalsbilaga 1. Tekniska krav v2.4.8
  - Implementationsprofilen eGov2 v2.0
  - Deploymentprofilen saml2int v0.1.2
  - Service and Attributes in SAML Metadata (SASM) v1.0.0



Följande dokument är deprekerade från och med 2023-03-08 och ska inte längre användas för nya implementationer.

Avtalsbilaga 1 – Tekniska krav:

- https://www.skolfederation.se/wp-content/uploads/2015/12/Bilaga-1-Tekniska-krav-v2_4_8.pdf

Implementationsprofilen eGov2 (beskriver vilka delar av SAML som måste implementeras):

- kantara-report-egov-saml2-profile-2.0

Deploymentprofilen saml2int (beskriver vilka delar av SAML som måste vara i bruk samt hur dessa ska användas):

- SAML2int Profile_v0.1.2.pdf

Profil som beskriver hur tjänster och attribut deklareras i SAML V2.0 metadata

- Services and Attributes in SAML Metadata.

Bakgrund

- Tidigare profiler och avtal som hänvisades till är gamla, och både på svenska och engelska
- Information i profiler och bilaga kunde överlappa – otydlighet i vad som gäller
- En ny version av saml2int har kommit, men den har inte fått det genomslag som tänktes och är inte normerande i andra federationer
- SWAMID och Sweden Connect skriver istället egna profiler inspirerade av men ej direkt hänvisande till saml2int

Vad innebär profilen?

- Krav på att den följs vid teknisk anslutning till Skolfederation
- Ej implementerat tvång i Federationsadmin – planerat under hösten 2023
- Innebär (främst) en del anpassning i metadata för medlemmar men också vissa funktioner i lösningar
- Vi går igenom några av kraven och diskuterar vad och varför

Några krav i urval

1. lang – språkdeklaration på engelska och svenska för alla tillämpbara element i metadata

Tidigare: bara krav på vissa element

Innebörd: anpassning av sitt metadata för både svenska och engelska värden (ex element Organization, ContactPerson, MDUI, AttributeConsumingService)

2. entityID

entityID måste vara i form av en URI (ex. https://example.com/idp)

Idag: många entiteter saknar rätt format på entityID (ex. ”skola-idp”, ”skola-skolfederation-sp”)

Innebörd: många entiteter kommer att behöva uppdatera sitt entityID för att överensstämma med profilen

3. errorURL

IdP behöver tillhandahålla en errorURL

Vid fel i inloggning, autentisering eller auktorisation kan en tjänsteleverantör hänvisa till en sida hos IdP’n som kan ge användaren ett lämpligt felmeddelande

Tidigare: inte kravställt

Innebörd: IdP’er kommer behöva ha en registrerad errorURL

4. Scope

Scope måste anges i metadata för IdP

Detta används för säkerhet vid användning av ”scopade attribut”, såsom ePPN

Tidigare: kravställt sedan hösten 2021

Nu: många som laddat upp MD innan hösten 2021 måste uppdatera sitt metadata med Scope (annars kommer inte inloggning till ex DNP att fungera)

5. MDUI

IdP’er måste tillhandahålla Metadata (...) and Discovery User Interface (MDUI)

Detta används för att bättre kunna anvisa användaren till rätt IdP i både centrala anvisningstjänster (ex Skolfeds, DNPs) men även ute i tjänsters lokala anvisningstjänster

Idag: OrganizationDisplayName har använts synonymt, vilket är en något felaktig workaround

Innebörd: IdP’er behöver lägga till MDUI i metadata: visningsnamn, beskrivning, logotyp

6. Attributdeklaration

IdP:s måste deklarera i metadata vilka attribut de stödjer att släppa
SP:s måste deklarera i metadata vilka attribut de efterfrågar

Inget nytt krav – men ej implementerat i Federationsadmin

Innebörd av krav: Ger möjlighet till god utveckling framöver!

Smidigare sammanställning av vilka attribut som krävs för åtkomst

Automatiska attributsläpp baserat på metadata – yay or nay?

7. Älskling, jag krympte metadatat

Enbart det som är essentiellt för federationens funktion kommer tillåtas och allt onödigt junk kommer att motas i metadatavalideringsgrind

Hejdå till större automatgenererade blaffor med gott och blandat (ex. ADFS)

Innebörd: Administratör får ta bort lite metadataelement innan uppladdning ☺

Några till i urval

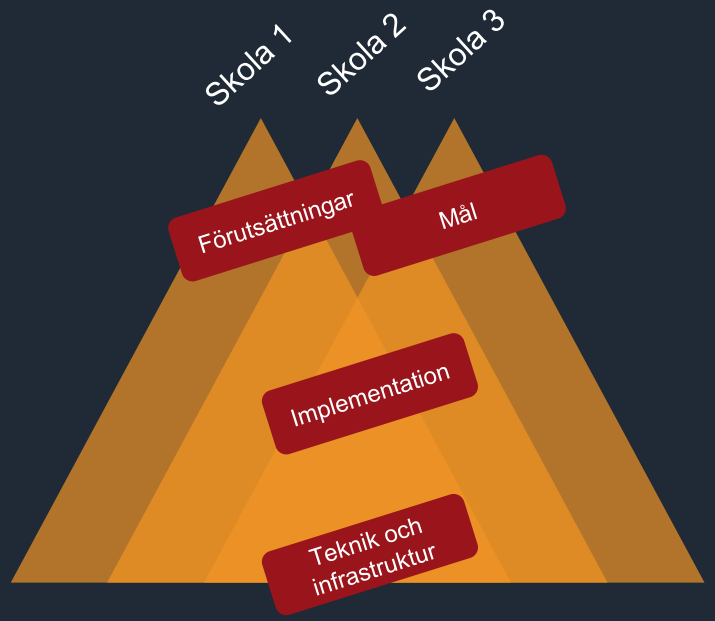
- Utgångna certifikat tillåts inte längre i metadata
- Metadata refresh – metadata måste hämtas varje timme av IdP/SP
  - Hur resonerar vi kring ex Google och Microsoft som saknar inbyggd funktionalitet för detta?
- Clock skew – klockor får helt enkelt inte gå för mycket fel
- Medlemmar får inte använda mjukvara eller bakomliggande infrastruktur med kända sårbarheter

Varför då alla dessa krav?

Denna förmiddag har vi fördjupat oss i standarder, implementationer, och funderat på olika val för att ta oss vidare.

Tydliga tekniska regelverk för *hur* vi gör de gemensamt överkomna aktiviteterna är av stor vikt.

Så specifikt som möjligt



Så delat som möjligt

Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkar för ett internet som bidrar positivt till människan och samhället.

INTERNET STIFTELSEN