Arbetsmöte
Sweden Connect Tekniskt ramverk

Martin Lindström – martin@idsec.se
Stefan Santesson - stefan@idsec.se

Agenda

- Presentation och bakgrund
- Föreslagna ändringar till Tekniskt ramverk
- Övriga specifikationer och standarder
- Andra federationer
- Arbetssätt
- Roadmap
- Öppna diskussioner

sweden connect

Föreslagna ändringar

- Finns som GitHub issues och pull requests på github.com/swedenconnect/technical-framework
- Diskussioner på Tekniskt forum - https://forum.eidasweb.se
- Saknas några önskemål?
- Inför nästa version hoppas vi att fler har bidragit.

sweden connect

Principal Selection (i)

- SAML har inget standardiserat sätt att skicka med känd identitet i AuthnRequest.
- Har varit ett problem för underskriftstjänster.
  - Har lett till olika mindre bra lösningar.
  - Vill helst inte prompta efter personnummer vid underskrift.
- Relevant för IdP:er som promptar efter personnummer.
- SHOULD inte MUST för IdP:er p.g.a. bakåtkompatibilitet.
  - Inför nästkommande version bör det vara MUST.

sweden connect

Principal Selection (ii)

```
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://test.swedenconnect.se/saml2/sign"
  Destination="https://idp-sweden-connect-valfr-2017.prod.frejaeid.com/idp/profile/SAML2/Redirect/SSO" ForceAuthn="true"
  ID="_d925a00e0f937087dd34cbfe640f3064" IsPassive="false" IssueInstant="2019-09-23T11:48:44.441Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Version="2.0">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://test.swedenconnect.se/sp-sign</saml2:Issuer>
  <saml2p:Extensions>
    <csig:SignMessage xmlns:csig="http://id.elegnamnden.se/csig/1.1/dss-ext/ns"
      DisplayEntity="https://idp-sweden-connect-valfr-2017.prod.frejaeid.com" MimeType="text" MustShow="true">
      <csig:EncryptedMessage>
        ...
      </csig:EncryptedMessage>
    </csig:SignMessage>
    <psc:PrincipalSelection xmlns:psc="http://id.swedenconnect.se/authn/1.0/principal-selection/ns">
      <psc:MatchValue Name="urn:oid:1.2.752.29.4.13"
        xmlns:psc="http://id.swedenconnect.se/authn/1.0/principal-selection/ns">19691129****</psc:MatchValue>
    </psc:PrincipalSelection>
  </saml2p:Extensions>
  <saml2p:RequestedAuthnContext Comparison="exact" xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
    <saml2:AuthnContextClassRef xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
      http://id.elegnamnden.se/loa/1.0/loa3-sigmessage</saml2:AuthnContextClassRef>
  </saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>
```

sweden connect

Ny version av SAML2Int

- kantarainitiative.github.io/SAMLprofiles/saml2int.html
- Är tyvärr lite väl ”bleeding edge” …
  - Subject Identifier Attributes
  - Avvecklande av NameID
  - Scopes
- Diskussion: Ska vi bygga på denna och göra undantag eller låta Tekniskt ramverk vara ”self-contained?”

sweden connect

Tydligare krav kring algoritmstöd

- Vi bör utgå från ”nya” SAML2Int.
- AES-GCM stöds inte av alla ännu, AES-CBC bör vara default ett tag till.
- RSA 1.5 för kryptering svartlistas.
- SHA-1 som digest i signaturer svartlistas.
- IdP:er skall stödja <md:EncryptionMethod> etc så att SP:ar kan begära användande av t.ex. AES-GCM.

sweden connect

Uncertified LoA 3

- BankID är inte granskat och godkänt för LoA 3.
- BankID IdP:er i Sweden Connect får använda uncertified-loa3 istället.
- Det finns installationer där BankID IdP:er använder LoA 3 i intyg ...
- Stöd i SP och underskriftstjänster ...

sweden connect

Entitetskategorier för avtal

- Alla IdP:er i Sweden Connect är inte tillgängliga för alla SP:ar. Avtalsstyrt.
- Valfrihetssystemet: http://id.swedenconnect.se/contract/sc/eid-choice-2017
- Leverantörsspecifika. T.ex.: http://id.swedenconnect.se/contract/Cybercom/Pensionsmyndigheten/Leveransavtal-SYS-2015-71
- Möjliggör Discovery Service-logik.

sweden connect

Uppdaterad BankID profil

- Regler för QR-kod.
  Önskat användande annonseras av SP mha entitetskategori i metadata – http://id.swedenconnect.se/general-ec/1.0/bankid/qr-code
- PrincipalSelection
- Rekommendationer för autostart-logik
- Rekommendationer för cancel

sweden connect

Annonserat algoritmstöd

- SAML v2.0 Metadata Profile for Algorithm Support Version 1.0 bör följas
- <md:EncryptionMethod>, <alg:DigestMethod>, <alg:SigningMethod>
- Möjliggör bättre interoperabilitet kring algoritmval
- Om AES-GCM stöds markera detta i metadata

sweden connect

Samordningsnummer

- Ej att likställa med personnummer
- Har endast betydelse för utfärdaren
- Fungerar inte i en nationell federation

sweden connect

Certifikatprofil för SignRequest

- Signeringscertifikat kan genereras enligt olika certifikatprofiler.
- Ett antal olika profiler definieras.
- Vilka profiler är aktuella?
- MUST eller SHOULD?

sweden connect

”Transaction evidence” i signeringscert

- https://github.com/swedenconnect/technical-framework/issues/69
- Lagra transaktions-ID i AuthContext i certifikatet
- Lagra SAD-payload i AuthContext i certifikatet

sweden connect

Övriga ändringar

- Språkfixar
- Uppdateringar av referensdokument
- Namnbyte: E-legitimationsnämnden -> Sweden Connect
- Introduktionsdokument översatt till engelska

sweden connect

Övriga specifikationer och standarder

- Normativa specifikationer för underskriftstjänst
  - Vara en del av Tekniskt ramverk?
- Federationsspecifika krav och regler
  - Idag lite rörigt angivna på swedenconnect.se
  - Knyta ihop tillitsramverk med Tekniskt ramverk
  - Regler kring loggning etc.
- Behövs en CPS, alternativt certifikatpolicy, för CA:n som finns i underskriftstjänster?

sweden connect

Andra federationer

- Hur förhåller sig Sweden Connect Tekniskt ramverk mot andra svenska federationer?
- Samverkan i syfte att likrikta och underlätta för integratörer och produktleverantörer?

sweden connect

Tekniskt ramverk – Nu och i framtiden

- Interoperabilitet i praktiken – Hur förbättrar vi oss?
- Stöd vid utveckling mot Tekniskt ramverk
  - Referensimplementationer
  - Samarbeten
  - Workshops
- Framtida arbetssätt
  - Mailing-lista?
  - Fler committers
  - Implementationer i gemensam testmiljö (sandbox)

sweden connect

Tekniskt ramverk – Roadmap

- Stöd för LoA 4 i SAML-federation
  - Holder of key eller motsvarande
- LoA 1 & 2?
  - Behöver vi göra något?
- Andra attributprofiler
- Bli av med sigmessage-URI:er
- Specifikationer för valideringsintyg och valideringstjänster
- Gemensamma API:er för stödtjänster?
- OpenID Connect

sweden connect