BILAGA 2 – Tekniska krav

Version 1.52

Innehåll

Revisionshistorik			
Version	**Datum**	**Författare**	**Kommentar**
1.0	2013-09-13	Staffan Hagnell	Redaktionella justeringar.
1.1	2014-02-11	Staffan Hagnell	Redaktionella justeringar.
1.2	2014-11-12	Staffan Hagnell	Ändrat från ”Bilaga 1” till ”Bilaga 2”.
1.3	2014-12-11	Robert Sundin	Utökad beskrivning av hantering av olika tillitsnivåer, samt redaktionella justeringar.
1.4	2015-02-24	Robert Sundin	-Specifika länkar till certifikat och metadata har ändrats till en generell hänvisning till Sambis webbplats. -Alternativet att verifiera nyckel via DNSSEC borttaget.
1.5	2015-08-26	Stefan Halén	Korrigerat stycket om hantering av olika tillitsnivåer, och justerat tillhörande scheman.
1.5	2015-08-26	Robert Sundin	Korrigerat transportskydd till enbart TLS i enlighet med RFC 7525.
1.5	2015-08-26	Robert Sundin	Specificerat krav för metadata från SP/IdP, samt federationens aggregerade metadata under stycket ”Utformning av metadata”.
1.5	2015-08-26	Robert Sundin	Infört krav på hur anvisningstjänst undviker sammanblandning av IdP:er.
1.5	2015-08-26	Robert Sundin	Infört krav på uppdateringsintervall för metadata (tolkning av cacheDuration/validUntil).
1.5	2015-08-26	Robert Sundin	Infört specificering av authnContext under identifieringsbegäran och identifieringssvar.
1.5	2015-08-26	Robert Sundin	Validering av AssertionConsumerServiceURL under identifieringsbegäran.
1.51	2015-12-22	Stefan Halén	Ändrat URL för dokumentation av LoA i schema.
1.52	2018-10-10	Eva Sartorius	Flyttat hit krypteringskrav från Tillitsramverket

Tekniska krav för anslutning till Sambi

Sambi har likt många andra Federativa initiativ som mål att använda följande SAML[1]-profiler:

- Implementationsprofilen eGov[2] 2.0 (beskriver vilka delar av SAML som måste implementeras)
- Deploymentprofilen saml2int[3] (beskriver vilka delar av SAML som måste vara i bruk samt hur dessa ska användas)

1 Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language 2.0 (SAML)
2 Kantara Initiative eGov 2.0 profile
3 Interoperable SAML 2.0 Web SSO deployment profile

De SAML-förmågor, där merparten är en del av implementationsprofilen eGov2, och hur SAML-förmågor påverkas av deploymentprofilen saml2int, redovisas övergripande i beskrivningen av den tekniska kravbilden i det följande.

Aktörskrav

Tjänsteleverantör (SP, Service Provider)

Tjänsteleverantören är ofta kravställare av identifieringsbegrepp, erfordrade Attribut samt Tillitsnivå (LoA, Level of Assurance).

Intygsutgivare (IdP, Identity Provider)

Intygsutgivare förutsätts ha tillgång till erforderliga register för att tillhandahålla de Attribut som efterfrågas av Tjänsteleverantören. Attribut kan innefatta personliga egenskaper eller andra uppgifter som ligger till grund för beslut om systembehörighet och åtkomstkontroll i förlitande e-tjänster.

Användare

I Sambi agerar varje Användare som tjänsteutövare, där denne representerar eller verkar hos en juridisk person.

Federationsoperatör

En av Federationsoperatörens viktigaste uppgifter är att tillhandahålla ett aggregat av digitalt signerat SAML-metadata, vilket kan anses vara Federationens tekniska kärna som knyter samman parterna.

Övergripande teknisk kravbild

Nyckelhantering

Säkerhetskrav på krypteringsnycklar

Samtliga Medlemmar i Federationen **ska,** själva eller med hjälp av underleverantör, skydda kryptografiskt nyckelmaterial, omfattande minst signeringsnycklar för:

a) metadata
b) identitetsintyg
c) kommunikation

Där annat inte angetts ska val av algoritmer och nyckellängder för autentisering, kryptering och signering följa NIST SP 800-131[4] eller ETSI TS 102 176-1[5]. I termer av algoritmval, kan dessa krav t.ex. uppfyllas genom att använda SHA-256 och RSA-nycklar med en nyckellängd (modulus) om minst 2048 bitar.

Observera att krav på nyckellängder och val av algoritmer är föremål för ständig omvärdering, varför detta krav kan komma att förändras över tid.

Publicering av Federationsoperatörens publika nyckel

Federationsoperatörens publika nyckel används för att verifiera signaturerna över publicerad SAML-metadata. Aktuell nyckel publiceras som en textfil på Sambis webbplats, www.sambi.se.

Verifiering av Federationsoperatörens publika nyckel

Vid uppdatering av den Federationsoperatörens publika nyckel i lokal konfiguration **ska** dess äkthet alltid verifieras mot minst två olika källor. Följande är sådana godtagbara verifieringskällor:

- hämtning av nyckel direkt från publiceringsplatsen (www.sambi.se), innefattande positiv verifiering av det certifikat som identifierar publiceringsplatsen.
- via kontakt med kundtjänst för att verifiera nyckelns digitala fingeravtryck över telefon (SHA-1 hex)

Byte av Federationsoperatörens publika nyckel

Vid planerat byte av Federationsoperatörens publika nyckel meddelas samtliga Federationens Medlemmar minst 30 dagar innan den nya nyckeln börjar att användas för signering. För att minska risken för sammanblandning publiceras den nya nyckeln på en webbadress som skiljer sig från tidigare nycklar enligt ovan.

Rutiner för byte av Medlemmars krypteringsnycklar

För byte av Medlems krypteringsnyckel **ska** följande steg genomföras:

1. Medlemmen förmedlar metadata innehållande den nya (publika) krypteringsnyckeln till Federationsoperatören för publicering.
2. Intill dess att den nya krypteringsnyckeln nått samtliga motparter inom Federationen **ska** Medlemmen använda dubbla nycklar för avkryptering.

4 http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf
5 http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02.01.01_60/ts_10217601v020101p.pdf

Rutiner för byte av Medlemmars signeringsnycklar

För byte av Medlems signeringsnyckel **ska** följande steg genomföras:

1. Medlemmen förmedlar metadata innehållande både den nya och den gamla (publika) signeringsnyckeln till Federationsoperatören för publicering.
2. Under en övergångsperiod **ska** samtliga motparter använda dubbla nycklar för verifiering av signaturers äkthet.
3. Då den nya nyckeln nått samtliga motparter inom Federationen **ska** Medlemmen förmedla uppdaterat metadata, innehållande endast den nya (publika) signeringsnyckeln till Federationsoperatören.

SAML-metadata (MD)

För att Medlemmarna i Federationen ska kunna lita på varandras intyg krävs ett utbyte av parternas publika nycklar som används för att verifiera t.ex. intygens signaturer.

Utbytet sker genom att lokalt SAML-metadata (MD), vilket beskriver en aktörs egenskaper, förmågor och publika nycklar, aggregeras av Federationsoperatören. Federationsoperatören genomför rimlighetskontroller, varefter denne signerar och publicerar det aggregerade SAML-metadatat. Det aggregerade och signerade SAML-metadata som publiceras av Federationsoperatören är således den samlade bilden av Federationens samtliga aktörers egenskaper, förmågor och publika nycklar.

Publicering av metadata

Federationens aggregerade och signerade SAML-metadata publiceras på Sambis webbplats, www.sambi.se

Verifiering av signerade metadata

Varje Medlem **ska,** med den av Federationsoperatören publicerade nyckeln, verifiera den elektroniska signatur som omsluter SAML-metadatat vid varje uppdatering av den lokala kopian.

Utformning av metadata

Sambi använder saml2int som *deploymentprofil* vilken beskriver hur SAML-metadata ska presenteras. Utformningen av SAML-metadata regleras i OASIS *SAML V2.0 metadata specification* [SAML2Meta[6]] och hantering av SAML-metadata regleras i OASIS *Metadata Interoperability Profile* [MetaIOP[7]]. Samtliga ingående Medlemmar i Federationen **ska** stödja dessa profiler.

6 http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
7 http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf

Gemensamma krav för SP och Idp Metadata. För samtliga <EntityDescriptor>, gäller att följande **ska** finnas:

- <Organization>, med <OrganizationName>, <OrganizationDisplayName> och <OrganizationURL> som har xml:lang="sv". <OrganizationDisplayName> **ska** vara enligt separat namnstandard.
- <ContactPerson> med contactType="technical" samt med contactType="support". Varje <ContactPerson> **ska** minst innehålla en <EmailAddress>. Supportkontakten avser support för andra federationsmedlemmar, samt som eskaleringsväg från 1st-line-support hos någon av federationsmedlemmarna.

För federationens aggregerade metadata gäller följande:

- metadata **ska** bestå av en <EntitiesDescriptor> rotnod som i sin tur innehåller <EntityDescriptor>-noder. Nästlade <EntitiesDescriptor>-noder **får inte** förekomma.
- cacheDuration och validUntil **ska** anges.

Uppdatering av metadata i lokal instans

Lokala instanser som använder federationens aggregerade metadata **bör** uppdatera data enligt angiven cacheDuration och **ska inte** betrakta metadata som tillförlitligt efter utgången validUntil.

Metadata **bör** uppdateras automatiskt enligt cacheDuration. Om hämtning misslyckas får gammalt metadata användas fram till tidpunkten som anges i validUntil. Därefter **ska** kommunikation med de idp/sp som listas i det utgångna metadatat inte längre tillåtas.

Anvisningstjänst (DS, Directory Service)

I grundscenariot där en Användare önskar använda en tjänst, mot vilken Användaren ännu inte är identifierad, blir denne ombedd att identifiera sig. I en tvåpartsrelation är det entydigt vilken Intygsutgivare som denne ska anvisa Användaren till. I en Federation likt Sambi med möjlighet till godtyckligt antal Intygsutgivare krävs därför en generisk funktion för att anvisa Användaren till ”sin” Intygsutgivare.
Anvisningstjänsten använder SAML-metadata för att visa Användaren de i Federationen ingående Intygsutgivarna.

Adress till den centrala anvisningstjänsten finns publicerad på Sambis webbplats, www.sambi.se.

En central Anvisningstjänst emellertid inte är en nödvändighet för samverkan inom Federationen. Tjänsteleverantören kan välja att implementera en egen funktion för lokal anvisning baserat på SAML-metadata.

Anvisningstjänst **ska** presentera IdPer så att det inte finns risk för sammanblandning mellan dessa. Vid risk för sammablandning **ska** OrganizationDisplayName presenteras.

Utöver grundscenariot finns även möjlighet att använda s.k. icke-ombedda intyg (*unsolicited response*), innebärande att Användaren först ansluter till sin Intygsutgivare med en parameter i anropet, som sedan användas för att anvisa Användaren till rätt E-tjänst.

Hantering av anvisning regleras av OASIS *Identity Provider Discovery Service Protocol Profile* [IdPDisco[8]]. Samtliga ingående Medlemmar i Federationen **bör** stödja denna profil.

Pseudonymiserade identitetsbegrepp (NameID)

En av Sambis hörnstenar är att ständigt värna om den personliga integriteten. Därför **bör**, i möjligaste mån, pseudonymer användas som identifieringsbegrepp (NameID).

Det finns två typer av pseudonymer. Dels *persistenta* pseudonymer vilka har egenskapen att de över tid alltid representerar samma Användare i den aktuella E-tjänsten, dels *transienta* pseudonymer vilka är tillfälliga och aldrig återanvänds.
Vid användning av persistenta pseudonymer presenteras olika pseudonymer för varje E-tjänst. Vid användning av transienta pseudonymer presenteras en ny pseudonym vid varje nytt tillfälle och för varje E-tjänst.

Pseudonymer är en del av standardspecifikationen för SAML 2.0 [SAML2Core[9]] och följande **ska** stödjas:

- urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
- urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Identifieringsbegäran

I grundscenariot där en Användare söker åtkomst till en E-tjänst, men ej redan är identifierad, blir denne ombedd att identifiera sig. Den begäran som E-tjänsten skapar i detta scenario är en identifieringsbegäran (AuthenticationRequest), vilken Användaren via ett hänvisningsanrop (SAML Redirect) tillhandahåller Intygsutgivaren.

8 http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf
9 http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

Sambi använder saml2int som *deployment profil* vilken beskriver hur *SAML V2.0 Web Browser SSO Profile* [SAML2Prof[10]] ska användas, vilket i sin tur återspeglas i identifieringsbegäran. I profilen föreskrivs även bland annat att:

- Intygsgivare **får** underlåta sig att verifiera signerade identifieringsbegäran om det kan antas att det föreligger risk för tillgänglighetsangrepp (Denial of Service, DoS) mot Intygsutgivningsfunktionen denna väg.

Specifika krav:

- Kommunikationen **ska** skyddas med TLS på transportnivå i enlighet med RFC 7525[11]
- <RequestedAuthnContext> **får** anges och **ska** i så fall sättas enligt [IAP] och [IANA LoA] med <AuthnContextClassRef> http://id.sambi.se/loa/loa3. Detta gäller tills vidare, så länge SAMBI bara stödjer LoA3.
- IdP **ska** validera att AssertionConsumerServiceURL stämmer med SP metadata.

Identifieringssvar

Identifieringssvaret kan vara en följd av en identifieringsbegäran, men det kan också vara ett svar utan någon föregående begäran. Den senare benämns icke-ombedda intyg (*unsolicited respons*)

Sambi använder saml2int som *deployment profil* vilken beskriver hur *SAML V2.0 Web Browser SSO Profile* [SAML2Prof] ska användas, vilket i sin tur återspeglas i identifieringssvaret.

I profilen föreskrivs bland annat:

- Identifieringssvaret **ska** signeras med en nyckel som är associerad med Intygsutgivaren i SAML-metadata.
- Tjänster **ska** acceptera icke-ombedda intyg (unsolicited response)
- Tjänster **ska** verifiera signaturer och dekryptera svar med någon av de giltiga nycklar som tjänsten har publicerad i SAML-metadata. Denna mekanism **ska** kunna användas vid byte av nycklar.
- Tjänster får inte använda eventuell giltighetstid för de certifikat som används som nyckelbärare i SAML-metadata som indikation på nyckelns giltighet – samtliga nycklar som finns tillgängliga i SAML-metadata **ska** betraktas som giltiga.
- Nycklar som inte ska användas ska tas bort från SAML-metadata.

Specifika krav

10 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

11 https://datatracker.ietf.org/doc/rfc7525/

- Kommunikationen **ska** skyddas med TLS på transportnivå i enlighet med RFC 7525[11]
- Om TLS inte kan tillämpas **ska** identifieringssvaret (AuthenticationResponse) krypteras i sin helhet med e-tjänstens publika nyckel som återfinns i SAML-metadata.
- <AuthnStatement> **ska** anges enligt [IAP]] och [IANA LoA] med <AuthnContextClassRef> satt till http://id.sambi.se/loa/loa3. Detta gäller tills vidare, så länge SAMBI bara stödjer LoA3.

Hantering av olika tillitsnivåer (LoA, Level of Assurance)

Sambi är en federation som hanterar flera olika tillitsnivåer i enlighet med tillitsramverket. Tjänsteleverantören är den som väljer tillitsnivå utifrån informationstillgångens skyddsvärde. Därför måste medlemmarna emellan kunna utbyta information om vilka tillitsnivåer som en intygsutfärdare kan erbjuda och vilken tillitsnivå som tjänsteleverantören kräver. Informationen om tillitsnivån kan dels adderas i SAML-metadata, dels inom ramen för en autentiseringsfråga och ett autentiseringssvar.

Information om tillitsnivå i SAML-metadata ger fördelen att anvisningstjänsten, som använder SAML-metadata för att presentera för användare lämpliga intygsutfärdare, kan begränsa presentationen till användare till att enbart presentera de intygsutfärdare som minst uppfyller den efterfrågade tillitsnivån.

I SAML-metadata representeras tillitsnivån av ett eller flera attribut. Samtliga ingående medlemmar **bör** hantera utökat SAML-metadata som tillåter presentation av attribut i enlighet med SAML V2.0 Metadata Extension for Entity Attributes Version 1.0[12] . Attributen för tillitsnivå presenteras i enlighet med SAML V2.0 Identity Assurance Profiles Version 1.0[13] och har följande benämningar:

- http://id.sambi.se/loa/loa2
- http://id.sambi.se/loa/loa3
- http://id.sambi.se/loa/loa4

Utbytet av informationen om tillitsnivå inom ramen för en autentiseringsfråga och ett autentiseringssvar ger möjlighet att hantera det faktum att en intygsutfärdare kan representeras av olika kategorier av användare där det inte är självklart att alla användare representerar samma tillitsnivå. Vidare kan en användare ha tillgång till olika autentiseringsmetoder som i sin tur kan representera olika tillitsnivåer. Utbytet av information sker inom ramen för Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0 [14]där varje tillitsnivå presenteras som en Authentication

[12] http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf

[13] http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.pdf

[14] http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

Context. Presentationen av tillitsnivåerna sker i enlighet med SAML V2.0 Identity Assurance Profiles.

Sambis tillitsnivåer refereras av en för varje nivå specifik URI som definierar autentiseringsklassen:

- http://id.sambi.se/loa/loa2
- http://id.sambi.se/loa/loa3
- http://id.sambi.se/loa/loa4

Denna URI återfinns i schemat som targetNamespace.

Attribut governingAgreementRef tillhörande element GoverningAgreement i schemat innehåller en URL som hänvisar till den externa dokumentation som definierar LOA nivån.

Signalering av tillitsnivåer i autentiseringsfrågor och autentiseringssvar **ska** hanteras inom ramen för AuthnContextClassRef.

En autentiseringsfråga **bör** signalera vilken tillitsnivå som krävs. Attributet [Comparison] **ska** sättas till ”exact” eller utelämnas då vissa SAML-mjukvaror endast har stöd för exakt matchning av <saml:AuthnContextClassRef>. Om [Comparison] utelämnas, **ska** det tolkas av intygsutfärdaren på samma sätt som ”exact” i enlighet med SAML-Core-2.0.

För att undvika problem för en användare som redan är autentiserad med en högre tillitsnivå än tjänsten kräver, **bör** autentiseringsfrågan innehålla samtliga tillitsnivåer som uppfyller tjänstens krav. En uppsättning av tillitsnivåer **ska** tolkas som en ordnad lista där det första elementet representerar den mest föredragna tillitsnivån.

Ett autentiseringssvar **ska** signalera den tillitsnivå som användaren autentiserats för. Om intygsutfärdaren inte kan matcha efterfrågad tillitsnivå, ska `<StatusCode> [urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext]` anges i svaret. Även oombedda autentiseringssvar (unsolicited response) **ska** signalera den tillitsnivå som användaren autentiserats för.

Det är alltid konsumenten av autentiseringssvaret som ansvarar för att göra en korrekt bedömning av tillitsnivåer i autentiseringssvaret. I det fall ett autentiseringssvar felaktigt saknar signalering av tillitsnivå, kan ingen nivå av tillit förutsättas.
Schema för respektive context class finns under http://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml och nedan i detta dokument.

sambi.se-loa2

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
   targetNamespace="http://id.sambi.se/loa/loa2"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xmlns="http://id.sambi.se/loa/loa2"
   finalDefault="extension"
   blockDefault="substitution"
   version="2.0">
  <xs:redefine schemaLocation="http://docs.oasis-
open.org/security/saml/v2.0/saml-schema-authn-context-types-2.0.xsd">
  <xs:annotation>
    <xs:documentation>
    Class identifier: http://id.sambi.se/loa/loa2 Defines Level 2 of the
Sambi.se Assurance Framework
    </xs:documentation>
  </xs:annotation>
  <xs:complexType name="AuthnContextDeclarationBaseType">
    <xs:complexContent>
    <xs:restriction base="AuthnContextDeclarationBaseType">
      <xs:sequence>
      <xs:element ref="GoverningAgreements"/>
      </xs:sequence>
      <xs:attribute name="ID" type="xs:ID" use="optional"/>
    </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="GoverningAgreementRefType">
    <xs:complexContent>
    <xs:restriction base="GoverningAgreementRefType">
      <xs:attribute name="governingAgreementRef"
      type="xs:anyURI"
      fixed="https://www.sambi.se/sambi-loa"
      use="required"/>
    </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
  </xs:redefine>
</xs:schema>
```

sambi.se-loa3

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
   targetNamespace="http://id.sambi.se/loa/loa3"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xmlns="http://id.sambi.se/loa/loa3"
   finalDefault="extension"
   blockDefault="substitution"
   version="2.0">
  <xs:redefine schemaLocation="http://docs.oasis-
open.org/security/saml/v2.0/saml-schema-authn-context-types-2.0.xsd">
  <xs:annotation>
    <xs:documentation>
    Class identifier: http://id.sambi.se/loa/loa3 Defines Level 3 of the
Sambi.se Assurance Framework
    </xs:documentation>
  </xs:annotation>
  <xs:complexType name="AuthnContextDeclarationBaseType">
    <xs:complexContent>
    <xs:restriction base="AuthnContextDeclarationBaseType">
      <xs:sequence>
      <xs:element ref="GoverningAgreements"/>
      </xs:sequence>
      <xs:attribute name="ID" type="xs:ID" use="optional"/>
    </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="GoverningAgreementRefType">
    <xs:complexContent>
    <xs:restriction base="GoverningAgreementRefType">
      <xs:attribute name="governingAgreementRef"
      type="xs:anyURI"
      fixed="https://www.sambi.se/sambi-loa"
      use="required"/>
    </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
  </xs:redefine>
</xs:schema>
```

sambi.se-loa4

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
   targetNamespace="http://id.sambi.se/loa/loa4"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xmlns="http://id.sambi.se/loa/loa4"
   finalDefault="extension"
   blockDefault="substitution"
   version="2.0">
  <xs:redefine schemaLocation="http://docs.oasis-
open.org/security/saml/v2.0/saml-schema-authn-context-types-2.0.xsd">
  <xs:annotation>
    <xs:documentation>
    Class identifier: http://id.sambi.se/loa/loa4 Defines Level 4 of the
Sambi.se Assurance Framework
    </xs:documentation>
  </xs:annotation>
  <xs:complexType name="AuthnContextDeclarationBaseType">
    <xs:complexContent>
    <xs:restriction base="AuthnContextDeclarationBaseType">
      <xs:sequence>
      <xs:element ref="GoverningAgreements"/>
      </xs:sequence>
      <xs:attribute name="ID" type="xs:ID" use="optional"/>
    </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="GoverningAgreementRefType">
    <xs:complexContent>
    <xs:restriction base="GoverningAgreementRefType">
      <xs:attribute name="governingAgreementRef"
      type="xs:anyURI"
      fixed="https://www.sambi.se/sambi-loa"
      use="required"/>
    </xs:restriction>
    </xs:complexContent>
  </xs:complexType>
  </xs:redefine>
</xs:schema>
```

Central utloggning (SLO, Single-logout)

Sambi ställer inledningsvis **inget** krav på att ingående Medlemmar ska stödja single-logout. Federationen sätter dock inte några hinder för att implementera single-logout.

Den tekniska specifikationen för att hantera single-logout inryms i *Single-logout Profile*[15]. Noterbart att själva sessionshanteringen inte är något som hanteras inom ramen för SAML viket gör frågan större än att bara vara en del i en teknisk specifikation.

Om en E-tjänst implementerar single-logout är det viktigt att det framgår i användargränssnittet att den är en single-logout som utförs och att det innebär en Användare loggas ur från (förhoppningsvis) alla tjänster där denna är inloggad.

Attribututgivare (AA, Attribute Authority*)*

Sambi erbjuder inte några för Federationen gemensamma Attribututgivartjänster.

Tid

Det är avgörande för Sambi att ingående Medlemmar använder en tillförlitlig källa för tid. Tidskällan **ska** vara spårbar till den svenska nationella tidsskalan UTC(SP)[16]. Detta bör realiseras med det standardiserade protokollet Network Time Protocol (NTP). Noggrannheten inom federationen bör aldrig avvika mer än en sekund.

15 http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
16 http://www.sp.se/sv/index/services/time_sync/ntp/Sidor/default.aspx