SAMBI SAML Profil

Samverkan för Behörighet och Identitet inom hälsa, vård och omsorg

Innehållsförteckning

Revisionshistorik			
Version	Datum	Författare	Kommentar
0.91	2012-06-29	Per Jonsson, Roger Öberg	Första utgåva
0.92	2012-07-02	Björn Skeppner	Redaktionella korrigeringar
1.0	2012-10-18	Per Jonsson, Roger Öberg	Initierande SLO begäran SKALL ske genom HTTP-Redirect alt HTTP-POST binding.
1.0.1	2012-10-20	Per Jonsson, Roger Öberg	Ändrade egenskapen caregiverid till careproviderid
1.0.2	2012-12-21	Per Jonsson, Roger Öberg	Förtydligat kraven på signering vid autentiseringsbegäran och svar. Uppdaterad matris-bild med krav på HTTP-POST för SP
1.03	2013-01-17	Björn Skeppner	Smärre textredigeringar
1.04	2013-03-04	Björn Skeppner	Smärre textredigeringar
1.1	2014-03-19	Björn Skeppner	Tagit bort kravet på signed request samt metadatakrav för SLO

1. Introduktion

Denna profil definierar ett urval av alla tekniker och lösningar som definieras av SAML. Syftet är att implementatörer kan anpassa sig enligt krav i denna profil, och på så sätt säkert erhålla interoperabilitet dem emellan.

Profilen är framtagen för att SAML Web SSO skall fungera i federerad miljö med olika produkter, så att sann Web SSO kan erhållas.

Profilen är en utökning på OASIS specifikationer gällande SAML V2.0 (se referenser). För att uppfylla denna profil SKALL alla krav i denna profil samt kraven som OASIS ställer i sina specifikationer (primärt SAML Web SSO profile) vara uppfyllda. Denna profil försöker inte upprepa sådana krav som finns i grundspecifikationerna.

Två existerande profiler har valts som arbetsunderlag för framtagandet av denna profil. Dessa är

- Kantara Initiative eGovernment Implementation Profile of SAML V2.0 [eGov2]
- Interoperable SAML 2.0 Web Browser SSO Deployment Profile [SAML2Int]

1.1. Specifikation

Identifikation: sambi-saml-profil

Kontaktinformation: Björn Skeppner, Inera

1.2. Notation

Tjänsteleverantör (Service Provider) benämns som SP genomgående i profilen.

Identifikationsleverantör (Identity Provider) benämns som IdP genomgående i profilen.

Senast vald IdP (om sådan finns) benämns som SSO IdP genomgående i profilen.

XML Element skrivs med typsnitt `Courier New`

```
<saml2p:AuthnRequest>
```

Hänvisning till referenser skrivs inom hakparenteser [referensidentifikation]

- SKALL är de krav som måste uppfyllas för att vara kompatibel med denna profil.
- KAN är de krav som är frivilliga, huruvida de uppfylls eller inte påverkar inte kompatibiliteten mot denna profil.
- BÖR är krav som rekommenderas att följas.

1.3. XML namnrymd

Följande namnrymder hanteras av profilen

Prefix	Namnrymd
saml2	urn:oasis:names:tc:SAML:2.0:assertion
saml2p	urn:oasis:names:tc:SAML:2.0:protocol
md	urn:oasis:names:tc:SAML:2.0:metadata
idpdisco	urn:oasis:names:tc:SAML:profiles:SSO:idp-disovery-protocol
mdattr	urn:oasis:names:tc:SAML:metadata:attribute
ds	http://www.w3.org/2000/09/xmldsig#

2. Metadata och förlitande hantering

SAML Metadata SKALL användas för att distribuera information mellan SAML-entiteter.

IdP och SP SKALL stödja SAML V2.0 Metadata Interoperability Profile Version 2.0 [MetaIOP]

IdP och SP SKALL stödja import och export av SAML V2.0 Metadata dokument.

IdP och SP BÖR stödja import och export av dokument genom följande metoder

- Filresurs
- Publicera och erhålla via "Well-Known Location", definierad av [SAML2Meta]

Implementationer BÖR stödja PKIX och OCSP/CRL för att säkerställa status på SAML entiteters certifikat, som används till ex. signering, server autentiserad SSL/TLS etc.

Implementationer KAN stödja ytterligare metoder för att säkerställa certifikat, ex. kontrollera certifikatets subjektnamn.

IdP och SP SKALL stödja metadatadokument vars rot-element är `<md:EntityDescriptor>` eller `<md:EntitiesDescriptor>`.

BÖR att vid uppdatering av nycklar ha med den äldre, samt den nya nyckeln i metadata dokumentet (i.e. två eller fler `<md:KeyDescriptor>`) för att få en smidig övergång.

2.1. IdP Metadata

IdP SKALL hantera metadata enligt följande

- SKALL finnas ett `<md:IDPSSODescriptor>` element.
- SKALL finnas minst en `<md:KeyDescriptor>` som innehåller ett `<ds:KeyInfo>` som i sin tur identifierar IdPs certifikat via `<ds:X509Certificate>`.
- BÖR finnas ett eller flera `<md:NameIDFormat>` som identifierar vilka namn-id format som stödjas.

2.2. SP Metadata

- Om [IdPDisco] används BÖR ett eller flera `<idpdisco:DiscoveryResponse>` finnas (under `<md:Extensions>` element), som beskriver vart IdP discovery svaret skall skickas. Om IdPDisco används och SP saknar `<idpdisco:DiscoveryResponse>` måste HTTP parameter för svaret anges enligt [IdPDisco].
- SKALL finnas ett `<md:SPSSODescriptor>` element.SKALL finnas minst en `<md:keyDescriptor>` som innehåller ett `<ds:KeyInfo>` som i sin tur identifierar SPs certifikat via `<ds:X509Certificate>`.
- BÖR finnas `<md:AttributeConsumerService>` som beskriver vilka tjänster SP tillhandhåller, samt dess egenskapsbehov.
- BÖR finnas `<md:SingleLogoutServic>` som beskriver vilka SLO-tjänster SP tillhandahåller (om sp:n stödjer SLO).
- BÖR finnas ett eller flera `<md:NameIdFormat>` som identifierar vilka namn-id format som stödjs.
- BÖR finnas ett `<md:ContactPerson>` element med egenskap ”`contactType`” satt till support och ytterligare ett `<md:ContactPerson>` element med egenskapen ”`contextType`” satt till `”techincal”`. `<md:ContactPerson>` BÖR innehålla minst ett `<md:EmailAddress>` element.

3. Namn-id format Följande namn-id format SKALL stödjas

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

4. Egenskaper

`<saml2:Attribute>` SKALL innehålla egenskapen `NameFormat` som är satt till `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.

`<saml2:AttributeValue>` BÖR endast innehålla en XML nod, som då är text.

4.1. Bas-egenskaper

Nedan specificeras alla bas-egenskaper som är definierade. Vissa egenskaper kan finnas med två gånger i utställt SAML-intyg (då även med det äldre namnet), för bakåtkompatibilitet. Viktigt dock att ta avstånd från dessa om möjligt

4.1.1. urn:sambi:names:attribute:authnMethod

Anger identifikationsmetod.

Möjliga värden:

`urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient` (Certifikat såsom SITHS)

`urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered` (OTP via sms)

Källa: IdP

4.1.2. urn:sambi:names:attribute:x509IssuerName

Anger utfärdare av certifkatet (t.ex SITHS) som användes vid identifikationen. Anges enbart om certifikat användes vid identifikationen.

Källa: Issuer ifrån certifkatet som användes vid identifikationen.

4.1.3. urn:sambi:names:attribute:levelOfAssurance

Anger tillåtsnivå(LoA)

Möjliga värden:

`urn:sambi:names:ac:classes:LoA1`

`urn:sambi:names:ac:classes:LoA2`

`urn:sambi:names:ac:classes:LoA3`

`urn:sambi:names:ac:classes:LoA4`

Källa: IdP

4.1.4. urn:sambi:names:attribute:title

HSA-titel för specificerad person.

Äldre namn: http://www.carelink.se/names/subject#legitimeradYrkestitel

Källa:
HSA-WS GetMiuForPerson
HSA-WS: hsaTitle
HSA: Legitimerad yrkesgrupp
LDAP: hsaTitle

4.1.5. urn:sambi:names:attribute:titleCode

Personens befattningskod

Äldre namn: http://www.carelink.se/names/subject#befattningskod

Källa: HSA-WS GetMiuForPerson
HSA-WS: paTitleCode

4.1.6. urn:sambi:names:attribute:personalPrescriptionCode

Förskrivarkod för specificerad person.

Äldre namn: http://www.carelink.se/names/subject#förskrivarkod

Källa: HSA-WS GetMiuForPerson
HSA-WS: personalPrescriptionCode
HSA: Förskrivarkod
LDAP: personalPrescriptionCode

4.1.7. urn:sambi:names:attribute:employeeHsaId

Användarens HSA-ID.

Äldre namn: http://www.carelink.se/names/subject#medarbetarid

Källa: SerialNumber ifrån SITHS-certifikatet eller ifrån HSA-WS GetMiuForPerson då autentisering sker med personnummer via engångslösenautentisering.

4.1.8. urn:sambi:names:attribute:givenName

Användarens förnamn.

Äldre namn: http://www.carelink.se/names/subject#förnamn
Källa: HSA-WS GetMiuForPerson
HSA-WS: givenName

4.1.9. urn:sambi:names:attribute:middleAndSurname

Användarens mellan- och efternamn

Äldre namn: http://www.carelink.se/names/subject#mellanOchEfternamn
Källa: HSA-WS GetMiuForPerson
HSA-WS: middleAndSurName

4.1.10. urn:sambi:names:attribute:commissionRight

Rättighet för aktuell uppdrag.

Äldre namn: http://www.carelink.se/names/subject#rättighetstyp
Källa: HSA-WS GetMiuForPerson
HSA-WS: miuRights
HSA: Medarbetaruppdragets rättigheter
LDAP: hsaCommissionRight

4.1.11. urn:sambi:names:attribute:commissionPurpose

Syfte med aktuell uppdrag

Äldre namn: http://www.carelink.se/names/subject#syftesbeskrivning
Källa: HSA-WS GetMiuForPerson
HSA-WS: miuPurpose
HSA: medarbetaruppdragets syfte
LDAP: hsaCommissionPurpose

4.1.12. urn:sambi:names:attribute:systemRole

Systemroller kopplade till specificerad användare.

Äldre namn: http://www.carelink.se/names/subject#systemRoll
Källa: HSA-WS GetMiuForPerson
HSA-WS: hsaSystemRoles
HSA: individuell behörighets-egenskap för it-tjänster
LDAP: hsaSystemRole

4.1.13. urn:sambi:names:attribute:assignmentHsaId

HSA-identitet för valt uppdrag.

Äldre namn: http://www.carelink.se/names/subject#uppdragsid
Källa: HSA-WS GetMiuForPerson
HSA-WS: hsaIdentity
HSA: HSA-id
LDAP: hsaIdentity

4.1.14. urn:sambi:names:attribute:assignmentName

Namn på valt uppdrag.

Äldre namn: http://www.carelink.se/names/subject#uppdragsnamn
Källa: HSA-WS GetMiuForPerson
HSA-WS: miuName
HSA: Objektnamn
LDAP: cn

4.1.15. urn:sambi:names:attribute:careUnitHsaId

HSA-identitet på den vårdenhet aktuellt uppdrag tillhör.

Äldre namn: http://www.carelink.se/names/subject#vårdenhetsid
Källa: HSA-WS GetMiuForPerson
HSA-WS: careUnitHsaIdentity
HSA: HSA-id
LDAP: hsaIdentity

4.1.16. urn:sambi:names:attribute:careUnitName

Namn på den vårdenhet aktuellt uppdrag tillhör.

Äldre namn: http://www.carelink.se/names/subject#vårdenhetsnamn

Källa: HSA-WS GetMiuForPerson
HSA-WS: careUnitName
HSA: Enhetsnamn eller Organisationsnamn
LDAP: ou eller o

4.1.17. urn:sambi:names:attribute:careProviderHsaId

HSA-identitet på den vårdgivare aktuellt uppdrag tillhör.

Äldre namn: http://www.carelink.se/names/subject#vårdgivarid

Källa: HSA-WS GetMiuForPerson
HSA-WS: careGiver
HSA: HSA-id

4.1.18. urn:sambi:names:attribute:careProviderName

Namn på den vårdgivare aktuellt uppdrag tillhör

Äldre namn: http://www.carelink.se/names/subject#vårdgivarnamn
Källa: HSA-WS GetMiuForPerson
HSA-WS: careGiverName
HSA: HSA-id
LDAP: ou eller o

4.2. Egenskaper när uppdrag saknas

Följande egenskaper medföljer även om aktören saknar uppdrag

- urn:sambi:names:attribute:authnMethod
- urn:sambi:names:attribute:x509IssuerName (endast vid autentisering genom certifikat)
- urn:sambi:names:attribute:levelOfAssurance
  urn:sambi:names:attribute:employeeHsaId (endast vid autentisering genom certifikat)Äldre namn: http://www.carelink.se/names/subject#medarbetarid

5. SSO IdP Identifiering

Detta kapitel identifierar metoder och tekniker som används för att identifiera SSO IdP.

Vid autentisering SKALL identifiering av aktör alltid göras mot den s.k. SSO IdP, detta för att erhålla sann Web SSO. För att göra detta finns tre möjliga alternativ.

- SP använder Identity Discovery Profile [SAML2Prof], d.v.s. common-domain cookie, för att erhålla aktörens SSO IdP.
- SP använder Identity Discovery Protocol and Profile [IdPDisco] för att erhålla aktörens SSO IdP.
- Om inget av ovan nämnda alternativ används kan SP använda en IdP som den vet agerar IdP proxy. Viktigt är dock att samma teknik används för att erhålla SSO IdP.

IdPDisco SKALL realiseras med tekniken common-domain cookie, enligt Identity Discovery Profile [SAML2Prof].

IdP proxy SKALL identifiera aktörens SSO IdP med en av de två förstnämnda metoder ovan.

Common-domain cookie SKALL vara transient.

Dessa krav resulterar i att ovan nämnda tre SSO IdP identifieringsmetoder är kompatibla med varandra.

6. Autentiseringsbegäran

6.1. Bindningar och säkerhetskrav

- SP SKALL stödja HTTP-Redirect bindning för utfärdande av begäran.
- IdP SKALL stödja HTTP-Redirect bindning för mottagande av begäran.
- IdP SKALL stödja SOAP bindning för mottagande av begäran.
- SSL/TLS SKALL användas för att säkra kommunikationen.

6.2. Begärans innehåll

SP KAN stödja, att delge vid behov, följande element

- `<saml2:AssertionConsumerServiceURL>` och `<saml2:ProtocolBinding>` eller `<saml2:AssertionConsumerServiceIndex>`.
  Om `<saml2:ProtocolBinding>` anges SKALL det vara satt till HTTP-Post alt HTTP-Artifact.
- `<saml2:ForceAuthn>`
- `<saml2:IsPassive>`
- `<saml2:AttributeConsumingServiceIndex>`
- `<saml2p:RequestedAuthnContext>`
- `<saml2p:NameIDPolicy>`
- `<saml2:Subject>`

IdP SKALL stödja alla ovan nämnda element som definieras av [SAML2Core].

IdP SKALL verifiera att begärande SP och angiven `<saml2p:AssertionConsumerService...>` är överensstämmande (med hjälp av SAML Metadata).

`<saml2p:AuthnRequest>` KAN innehålla ett `<saml2:Subject>`, huruvida IdP använder det eller inte är upp till IdP.

IdP som agerar proxy SKALL stödja `<saml2p:AuthnRequest>` som inte innehåller ett `<saml2p:Scoping>` element. Proxy IdPns `<saml2p:AuthnRequest>` KAN innehålla ett `<saml2p:Scoping>` element, fastän den initiala begäran inte hade det.

Om `<saml2p:RequestredAuthnContext>` anges BÖR egenskapen ”`comparison`” vara satt till ”`exact`”.

7. Autentiseringssvar

7.1. Bindningar och säkerhetskrav

- SP SKALL stödja HTTP-Post, alternativt HTTP-Artifact för mottagande av svaret.
- IdP SKALL stödja HTTP-Post för utfärdande av svaret.
- SP KAN stödja HTTP-Artifact för mottagande av svaret (se HTTP-Artifact kaptiel nedan).
- IdP SKA stödja HTTP-Artifact för utfärdande av svaret (se HTTP-Artifact kapitel nedan).
- SP SKALL säkra HTTP-Post URL med SSL/TLS.
- `<saml2:EncryptedId>` och `<saml2:EncryptedAttribute>` BÖR inte användas.
- IdP SKALL signera `<saml2:Assertion>` elementet (alltså inte `<saml2:Response>` elementet).
- SP och IdP SKALL hantera ”unsolicitated responses”
- SSL/TLS SKALL användas för att säkra kommunikationen.

7.2. HTTP-Artifact

Om HTTP-Artifact används måste följande följas.

- SKALL stödja ”Artifact resolution” enligt [SAML2Prof]
- SOAP SKALL användas för `<saml2p:ArtifactResolve>` och `<saml2p:ArtifactResponse>`.
- Artifakt format `urn:oasis:names:tc:SAML:2.0:artifact-04` SKALL stödjas, definierat i [SAML2Prof].

7.3. Svarets innehåll

- `<saml2:Respnose>` SKALL innehålla maximalt en `<saml2:Assertion`, en `<saml2:AuthnStatement>` och en `<saml2:AttributeStatement>`
- `<saml2:Subject>` KAN innehålla ett `<saml2:NameID>`.
- SP SKALL verifiera att signaturen på `<saml2:Assertion>` elementet är korrekt (med hjälp av SAML Metadata).

8. IdP som Proxy

8.1. Autentiseringsbegäran

- SKALL stödja mappning mellan inkommande och utgående `<saml2:RequestedAuthnContext>` och `<saml2:NameIDPolicy>`.
- SKALL stödja att man kan ”dölja” `<saml2:RequesterID>` från utgående `<saml2:AuthnRequest>`.

8.2. Autentiseringssvar

- SKALL stödja mappning mellan inkommande och utgående `<saml2:AuthnContext>` och `<saml2:NameIDPolicy>`.
- SKALL stödja att man kan ”dölja” `<saml2:AuthenticatingAuthority>` element från utgående `<saml2:AuthnContext>`.

9. Koordinerad utloggning (SLO)

Initierande begäran SKALL skickas över front-channel bindnig (HTTP-Redirect alt HTTP-POST). Propagerande av begäran/svar sker på respektive SP föredragen bindning (med hjälp av metadata).

9.1. Utloggningsbegäran

Efterföljande utloggningsbegäran mellan IdP och de SP som är autentiserade i samma session kan ske över back-channel(SOAP) eller front-channel(HTTP-Redirect/HTTP-POST).

Back-channel propagering har större fördelar än front-channel, eftersom det bedöms som mer troligt att lyckas med koordinerad utloggning. Front-channel är känslig i och med att aktörens webb-läsare identifierar för många omdirigeringar (redirects) som ett fel. Webb-läsaran kan då visa ett fel för användaren istället för att tillåta omdirigeringen. En annan nackdel med front-channel är att aktören kan stänga webb-läsaren innan alla meddelanden har propagerats, och således erhålls inte fullständig koordinerad utloggning.

Nackdelen med back-channel är att det ställer krav på SP, som ex vid lastbalanserade lösningar måste dela sessionsdata, avseende inloggning. Utöver måste SP hålla någon form av mappning mellan aktörer (alt SSO sessionsindex) och dess webbsessioner..

Om front-channel används är REKOMMENDATION att SP BÖR använda HTTP-POST bindning framför HTTP-Redirect för att undvika problemet med för många omdirigeringar.

9.2. Bindning och säkerhetskrav

- IdP SKALL stödja HTTP-POST och HTTP-Redirect för utfärdande och mottagande av `<saml2p:LogoutRequest>`.
- SP SKALL stödja HTTP-POST för utfärdande och mottagande av `<saml2p:LogutRequest>`.
- IdP KAN stödja SOAP för utfärdande och mottagande av `<saml2p:LogoutRequest>`.
- SP KAN stödja SOAP för utfärdande och mottagande av `<saml2p:LogoutRequest>`.
- SSL/TLS SKALL användas för att säkra kommunikationen.

9.3. Webb-läsare (User Agent)

- IdP SKALL stödja aktörs-initierad utloggning.
- IdP SKALL informera aktören om att endast delvis utloggning var möjlig. Då genom att returnera ett `<saml2p:LogoutResponse>` element med korrekt status-kod.
- IdP SKALL tillåta administrativ utloggning av aktörer.
- SP SKALL tillåta aktörs-initierad utloggning.

9.4. Loggoutsvar

- IdP SKALL stödja SOAP bindning och HTTP-Redirect för utfärdande av `<saml2p:LogoutResponse>`.
- IdP SKALL stödja HTTP-POST och SOAP bindning för mottagande av `<saml2p:LogoutResponse>`.
- SP SKALL stödja HTTP-Redirect och/eller SOAP för både utfärdande och mottagande av `<saml2p:LogoutResponse>`.
- SSL/TLS SKALL användas för att säkra kommunikationen.

10. Identifikation av aktör (och uppdragsval)

Definierar mekanismer för att hantera identifiering av aktören, samt ev. uppdragsval.

För att byta uppdrag SKALL en SLO begäran göras (som avslutar SSO sessionen), för att sedan på nytt autentisera aktören (då uppdrag måste väljas).

- IdP SKALL identifiera aktören.
- IdP SKALL säkerställa att aktören är upplagd i HSA-katalogen, genom anrop till HSA-WS. Om aktören inte är upplagd SKALL ett `<saml2p:Response>` med följande felkod returneras.
  - `urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal`
- IdP SKALL, om aktören inte har en giltig SSO session, hämta aktörens alla uppdrag från HSA-katalogen, genom anrop till HSA-WS. Uppdragsval SKALL hanteras enligt följande:
  - Inga uppdrag funna, autentisering skall fortgå.
  - Ett uppdrag funnet. Det uppdraget SKALL väljas automatiskt.
  - Två eller flera uppdrag funna. Aktören SKALL presenteras en ”välj uppdrag” dialog, där aktören aktivt väljer uppdrag.
- IdP SKALL vid `forceAuthn` satt till `TRUE` endast identifiera aktören på nytt, INTE presentera uppdragsval (förutsatt att aktören redan har en giltig SSO session).

11. Authentication Context (AuthnContext)

Detta kapitel definierar AuthnContext tillitsnivå (assurance level), enligt [IAFAL]. Tillitsnivån medföljer utställt SAML-intyg (se kapitel Egenskaper).

11.1. Tillitsnivåer (LoA)

Följande tillitsnivåer definieras av denna profil:

Tillitsnivå LoA1

Låg tillit till en aktörs identitet.

Identifikation: `urn:sambi:names:ac:classes:LoA1`

Tillitsnivå LoA2

Viss tillit till en aktörs identitet.

Identifikation: `urn:sambi:names:ac:classes:LoA2`

Tillitsnivå LoA3

Hög tillit till en aktörs identitet.

Identifikation: `urn:sambi:names:ac:classes:LoA3`

Tillitsnivå LoA4

Mycket hög tillit till en aktörs identitet.

Identifikation: `urn:sambi:names:ac:classes:LoA4`

11.2. Identifikationsmetoder

Nedan definieras de identifikationsmetoder som initialt behöver stödjas. Aktuell identifikationsmetod medföljer utställt SAML-intyg (se kapitel Egenskaper).

SSL/TLS Certificate-Based Client Authentication

Identifikation: `urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient`

Tillitsnivå: LoA3

Krav: SKALL stödjas av IdP. Denna AuthnContext används för att autentisera aktören genom dess X.509 certifikat (ex SITHS).

MobileTwoFactorUnregistered

Identifikation: `urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered`

Tillitsnivå: LoA3

Krav: KAN stödjas av IdP. Denna AuthnContext används för att autentisera aktören med hjälp av dess mobiltelefon (ex OTP).

12. Feature Matrix

Färg	Beskrivning
	Denna profil överensstämmer med [SAML2Conf]
	Denna profil definierar detta som frivilligt
	Denna profil tar inte ställning till dessa

Table 2: Feature Matrix

Feature	IdP	IdP Lite	SP	SP Lite	ECP
Web SSO, <AuthnRequest>,HTTP redirect	MUST	MUST	MUST	MUST	N/A
Web SSO, <Response>, HTTP POST	MUST	MUST	MUST	MUST	N/A
Web SSO, <Response>, HTTP artifact	MUST	MUST	MUST	MUST	N/A
Artifact Resolution, SOAP	MUST	MUST	MUST	MUST	N/A
Enhanced Client/Proxy SSO, PAOS	MUST	MUST	MUST	MUST	MUST
Name Identifier Management,HTTP redirect (IdP-initiated)	MUST	MUST NOT	MUST	MUST NOT	N/A
Name Identifier Management, SOAP (IdP-initiated)	MUST	MUST NOT	OPTIONAL	MUST NOT	N/A
Name Identifier Management, HTTP redirect	MUST	MUST NOT	MUST	MUST NOT	N/A
Name Identifier Management, SOAP (SP-initiated)	MUST	MUST NOT	OPTIONAL	MUST NOT	N/A
Single Logout (IdP-initiated) – HTTP redirect	MUST	MUST	MUST	MUST	N/A
Single Logout (IdP-initiated) – SOAP	MUST	OPTIONAL	MUST	OPTIONAL	N/A
Single Logout (SP-initiated) – HTTP redirect	MUST	MUST	MUST	MUST	N/A
Single Logout (SP-initiated) – SOAP	MUST	OPTIONAL	MUST	OPTIONAL	N/A
Identity Provider Discovery (cookie)	MUST	MUST	OPTIONAL	OPTIONAL	N/A

13. Kryptering/Signering

[SAML2Conf] definierar SHA-1 hash algoritm som SKALL. Med hänseende till den matematiska svaghet som identifierades 2005, används den starkare hash algoritmen SHA-2 (SHA256) där det är möjligt.

Enligt [SAML2Conf] ska implementationer som använder Web SSO profilen stödja följande SSL/TLS algoritmer.

SSL-kompatibla implementeringar måste förhålla sig till följande

- SKALL `SSL_RSA_WITH_3DES_EDE_CBC_SHA`

TLS-kompatibla implementeringar måste förhålla sig till följande

- SKALL `TLS_RSA_WITH_3DES_EDE_CBC_SHA`
- BÖR `TLS_RSA_AES_128_CBC_SHA`
- BÖR `TLS_RSA_AES_256_CBC_SHA`

13.1. XML

13.1.1. Signaturalgoritmer

Digest: SKALL `SHA256`

MAC: SKALL `HMAC-SHA256`

XML canonicalization: SKALL CanonicalXML (without comments)

Transform: SKALL Enveloped signature

Signature: SKALL `RSAwithSHA256`

Signature: BÖR `DSAwithSHA256`

13.1.2. Krypteringsalgoritmer

Block Encryption: SKALL `TRIPLE DES`, `AES-128`, `AES-256`

Key Transport: SKALL `RSA-v1.5`, `RSA-OAEP`

14. Termer

Förkortning	Beskrivning
SP	Service Provider, Tjänsteleverantör
IdP	Identity Provider, Autentiseringstjänst
SLO	Single Logout
SSO	Single Sign On
SAML2Bind	
SAML2Conf	
SAML2Err	
SAML2Meta	
IdPDisco	
MetaIOP	
XMLEnc	
XMLDSig	
Tillitsnivå	Tillitsnivå; den skyddsklass till vilken en elektronisk legitimation hänförs.

15. Referenser

Referens	Hänvisning
eGov	
SAML2Int	
SAML2Core	
SAML2Prof	
SAML2Bind	
SAML2Conf	
SAML2Err	
SAML2Meta	
IdPDisco	

MetaIOP	
XMLEnc	
XMLDSig	
IAFAL	Identity Assurance Framework:Assurance Levels

16. Bilaga 1

16.1. Avsteg från arbetsunderlaget

Följande kapitel specificerar en delmängd avsteg, alternative tillägg, som är gjorda mot de båda profiler som ligger till grunden för denna profil. För tydliga specifikationer gällande denna profil, se respektive kapitel.

- [eGov2] definierar publicering samt erhålla SAML metadata från ”Well-Known Location” som SKALL, denna profil definierar detta som BÖR.
- [eGov2] definierar IdPDisco som SKALL. [SAML2Int] definierar endast att om den används SKALL `<idpdisco:DiscoveryResponse>` inkluderas i metadata för SP, denna profil definierar detta som KAN.
- [SAML2Int] definierar att `<md:ContactPerson>` BÖR finnas. [eGov2] hanterar inte detta. Denna profil väljer att följa [SAML2Int].
- [eGov2] definierar HTTP-Artifact bindning som SKALL, denna profil har BÖR.
- [SAML2Int] BÖR, medans [eGov2] SKALL säkerställa att `<saml:AssertionConsumerServiceURL>` alt `<saml:AssertionConsumingServiceIndex>` är korrekta enligt SPs metadata. Denna profil har SKALL.
- [SAML2Int] definierar att `<saml2p:AuthnRequest>` SKALL INTE innehålla `<saml2:Subject>`. Se kapitel namn-id format, samt autentiseringsbegäran för denna profils definition.
- [SAML2Int] hanterar inte koordinerad utloggning. Denna profil rättar sig enligt [eGov2], förutom ställningstagande gällande utloggning från lokal alt global session.