BILAGA 1

Tekniska krav

Version 2.4.8

Tekniska krav för anslutning till Skolfederation

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

- eGov[2] 2.0
- saml2int[3], the Interoperable SAML 2.0 Profile

I denna bilaga redovisas ett urval av de viktigare SAML-förmågor som hämtats från implementationsprofilen eGov2 och de krav som saml2int ställer på dem.

Aktörskrav

Tjänsteleverantör (SP, Service Provider)

Med Tjänsteleverantör avses en part som tillhandahåller en tjänst som Användare får tillgång till baserat på av Intygsutgivare utfärdade intyg. Tjänsteleverantören är ofta kravställare av identifieringsbegrepp, erfordrade Attribut samt Tillitsnivå (LoA, Level of Assurance).

Intygsutgivare (IdP, Identity Provider)

Med Intygsutgivare avses den Användarorganisation eller motsvarande som tilldelar Användare elektroniska identiteter och Attribut samt utfärdar intyg baserat på dessa

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 Browser SSO Deployment Profile, http://saml2int.org/

inom Skolfederation. Intygsutgivaren förutsätts ha tillgång till erforderliga register för att tillhandahålla de Attribut som efterfrågas av Tjänsteleverantören.

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. Federationsoperatören ansvarar för att annoteringar och utökningar i metadata som registrerats direkt hos Skolfederation är korrekt och i den mån dessa påverkar beteende hos Intygsutgivare och Tjänsteleverantörer också överensstämmer med federationens regelverk och gällande lag.

Övergripande teknisk kravbild

Nyckelhantering

Säkerhetskrav på nycklar för signering och kryptering

Samtliga Medlemmar i Federationen **ska** skapa, hantera och förvara sina signerings- och krypteringsnycklar i enlighet med de krav som ställs i Skolfederations Tillitsramverk.

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 kraven uppfyllas genom att använda SHA-256 och RSA 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 verifiera signaturerna över publicerad SAML-metadata. Aktuell nyckel publiceras som ett certifikat under följande webbadress:

- https://www.skolfederation.se/certifikat-for-metadata-skolfederation/

Verifiering av Federationsoperatörens publika nyckel

Vid uppdatering av Federationsoperatörens publika nyckel i en Medlems lokala konfiguration **ska** Medlemmen alltid verifiera dess äkthet mot minst två olika källor.

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

Följande är sådana godtagbara verifieringskällor:

- hämtning av nyckel direkt från publiceringsplatsen (https://www.skolfederation.se/certifikat-for-metadata-skolfederation), innefattande positiv verifiering av det HTTPS- certifikat som identifierar publiceringsplatsen (i enlighet med Web PKI),
- kontakt med Skolfederations kundtjänst, där nyckelns digitala fingeravtryck verifieras över telefon.

Byte av Federationsoperatörens publika nyckel

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

Rutiner för byte av Medlemmars krypteringsnycklar

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

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

Om ovanstående steg inte genomförs riskeras avbrott i tjänsten intill dess att samtliga motparter inom Federationen hämtat samt börjat använda aktuellt metadata.

Rutiner för byte av Medlemmars signeringsnycklar

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

1. Medlemmen förmedlar SAML-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 **bör** Medlemmen förmedla uppdaterat SAML-metadata, innehållande endast den nya (publika) signeringsnyckeln till Federationsoperatören.

Om ovanstående steg inte genomförs riskeras avbrott i tjänsten intill dess att samtliga motparter inom Federationen hämtat samt börjat använda aktuellt metadata.

SAML-metadata (MD)

För att Medlemmarna i Federationen ska kunna lita på varandras intyg krävs ett utbyte av parternas publika nycklar. Utbytet sker genom att Medlemmarnas SAML-metadata (MD), vilket beskriver deras 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 SAML-metadata

Federationens aggregerade och signerade SAML-metadata publiceras under följande adress (VERSION ersätts med versionsnummer för aktuellt metadata):

- https://fed.skolfederation.se/prod/md/skolfederation-VERSION.xml

Verifiering av signerad SAML-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 SAML-metadata

I saml2int beskrivs 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.

Uppdatering av Skolfederations metadata

Skolfederations metadata innehåller beskrivning av hur länge det får användas via attributen *cacheDuration* och *validUntil* på elementet *EntitiesDescriptor* (normalt det första elementet i SAML-metadata). Medlem skall normalt uppdatera sin lokala kopia av federationens metadata åtminstone med den periodicitet som anges i *cacheDuration*. Beroende på val av programvara sker detta automatiskt.

Anvisningstjänst (DS, Directory Service)

När 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

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

likt Skolfederation med möjlighet till ett stort antal Intygsutgivare krävs däremot en generisk funktion för att anvisa Användaren till ”sin” Intygsutgivare.

Anvisningstjänsten använder SAML-metadata för att visa Användaren de i Federationen ingående Intygsutgivarna.

Federationens centrala anvisningstjänst finns under adressen:

- https://fed.skolfederation.se/prod/ds/

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

En annan möjlighet är 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 Skolfederations 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 permanenta (*persistent)* pseudonymer vilka har egenskapen att de över tid alltid representerar samma Användare i den aktuella E-tjänsten, dels icke-permanenta *(transient)* pseudonymer vilka är tillfälliga och aldrig återanvänds.

Vid användning av permanenta pseudonymer presenteras olika pseudonymer för varje E-tjänst. Vid användning av icke-permanenta 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

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

Identifieringsbegäran

När en Användare söker åtkomst till en E-tjänst, men inte 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 sin Intygsutgivare.

I saml2int föreskrivs hur *SAML V2.0 Web Browser SSO Profile* [SAML2Prof[10]] ska användas och däribland identifieringsbegäran. I profilen föreskrivs bland annat att:

- Kommunikationen **ska** skyddas med TLS/SSL på transportnivå.
- Intygsgivare **får** underlåta sig att verifiera signerade identifieringsbegäran om det kan antas att det föreligger risk för tillgänglighetsangrepp (Denial of Service, DoS) mot Intygsutgivnings-funktionen via denna väg.

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 response*).

I saml2int föreskrivs hur *SAML V2.0 Web Browser SSO Profile* [SAML2Prof] ska användas, och däribland identifieringssvar. I profilen föreskrivs bland annat:

- Kommunikationen **ska** skyddas med TLS/SSL på transportnivå.
- Om TLS/SSL inte kan tillämpas **ska** identifieringssvaret (*AuthenticationResponse*) krypteras i sin helhet med e-tjänstens publika nyckel som återfinns i SAML-metadata.
- 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.

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

Hantering av olika Tillitsnivåer (LoA, Level of Assurance)

Skolfederation avser att kunna hanterar flera olika Tillitsnivåer i enlighet med dess Tillitsramverk. Tjänsteleverantören har då möjlighet att välja Tillitsnivå utifrån de risker som är förknippade med e-tjänsten. Därför **bör** Medlemmarna kunna utbyta information om vilka Tillitsnivåer som en Intygsutgivare kan erbjuda och vilken Tillitsnivå som Tjänsteleverantören kräver. Informationen om Tillitsnivån kan dels läggas till i SAML-metadata, dels inom ramen för en identifieringsbegäran och ett identifieringssvar.

Tillitsnivåer i SAML-metadata

Information om Tillitsnivå i SAML-metadata ger fördelen att Anvisningstjänsten kan begränsa urvalet av Intygsutgivare till att för Användaren enbart presentera de som uppfyller den efterfrågade Tillitsnivån eller högre.

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*[11]. Attributen för Tillitsnivå presenteras i enlighet med *SAML V2.0 Identity Assurance Profiles*[12] och har följande benämning:

- http://id.skolfederation.se/loa/bas
- http://id.skolfederation.se/loa/2fa
- http://id.skolfederation.se/loa/loa2
- http://id.skolfederation.se/loa/loa3

Tillitsnivåer i identifieringsbegäran och svar

Utbytet av informationen om Tillitsnivå i en identifieringsbegäran och identifieringssvar ger möjlighet att hantera Användare med olika Tillitsnivåer. En och samma Användare kan även ha tillgång till olika elektroniska ID-handlingar med olika Tillitsnivåer. Utbytet av information sker inom ramen för *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*[13]. Presentationen av Tillitsnivåerna sker i enlighet med *SAML V2.0 Identity Assurance Profiles*.

Skolfederations Tillitsnivåer presenteras som *governingAgreementRef* Attribut under elementet *GoverningAgreement* i *Authentication Context* och har följande benämningar:

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

12 http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-01.pdf

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

- http://id.skolfederation.se/loa/bas
- http://id.skolfederation.se/loa/2fa
- http://id.skolfederation.se/loa/loa2
- http://id.skolfederation.se/loa/loa3

Avsaknad av stöd för hantering av Tillitsnivåer

Samtliga Medlemmar **bör** stödja utbyte av informationen om Tillitsnivå i SAML-metadata och i identifieringsbegäran och identifieringssvar.

Medlemmar som **inte** har stöd att hantera olika Tillitsnivåer enligt ovan **ska** då anses tillhöra Tillitsnivå http://id.skolfederation.se/loa/bas.

Central utloggning (SLO, Single-logout)

Skolfederation 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*[14]. Det bör noteras 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 att en Användare loggas ur från (förhoppningsvis) alla tjänster där denna är inloggad.

Attribututgivare (AA, Attribute Authority)

Skolfederationen bygger likt flertalet andra federationer på en decentraliserad attributsförsörjning där försörjningen i huvudsak sker genom intygsutfärdaren (IdP). En federation kan också innehålla centrala attributstjänster (*AA, Attribute Authorities*). Federationsoperatören erbjuder för närvarande inte några centrala attributstjänster (AA). Det finns emellertid inte några infrastrukturella hinder för att etablera sådana gemensamma Attribututgivartjänster inom ramen för Skolfederation.

Tid

Det är avgörande för Skolfederation att ingående Medlemmar använder en tillförlitlig källa för tid. Tidskällan **ska** vara spårbar till den svenska nationella tidsskalan

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

UTC(SP)[15]. Detta bör realiseras med det standardiserade protokollet Network Time Protocol (NTP). Noggrannheten inom Federationen bör aldrig avvika mer än en sekund.

15 http://www.sp.se/sv/index/services/time_sync/ntp/