# Utveckling av Skolfederations tillitshantering

Tid: 2013-12-11, kl 13.00

Plats: .SE, Ringvägen 100

Telefon: 08—999212, möteskod 322134

Närvarande:

erling.sjostrom@tieto.com
fredrik@kirei.se
jorgen.hellgren@e-identitet.se
kristinaedman@telia.com
lennart.henriksson@skola.sundsvall.se
Robert.Sundin@iis.se
Staffan.Hagnell@iis.se

Förhindrade:

bjorn.bergqvist@intraservice.goteborg.se
Emma Dahlström, eda@condidact.se
girgen@pingpong.net
hans.nilsson@taby.se
jonas.ryberg@unikum.net
magnus.berglund@unikum.net
peter.lundberg@intraservice.goteborg.se
stefan.runneberger@nexusgroup.com
ulf.solberg@stockholm.se
Ulrich.Wisser@iis.se

## Agenda

1. Godkännande av agendan
2. Avrapportering av arbetet med att ta fram en LoA-kravnivå lämplig för skolan
3. Hantering och signalering av den nya kravnivån
4. Övriga frågor
5. Nästa möte

## Uppdragspunkter

- Kan Skolfederation sätta upp en test IdP som har möjlighet att signalera de olika tillitsnivåerna?
- Staffan Hagnell undersöker vad som finns och möjligheterna för .SE att ta fram mallar för personuppgiftsbiträdesavtal.
- Ta fram ett till förenklat tillitsramverk ”LoA Skolfederation 2013” till nästa möte.

# 1 Godkännande av agendan

Den föreslagna agendan godkändes utan tillägg.

# 2 Arbetet med en LoA-kravnivå lämpliga för skolan

## 2.1 Underlag utsänd innan mötet

Ett arbete har inletts för att vidareutveckla Skolfederations ramverk. Målsättningen är att Skolfederation inte ska gå en egen väg utan ha samma inriktning som Sambi (Samverkan för behörighet och identitet inom hälsa, vård och omsorg) och E-legitimationsnämnden (den kommande Svensk E-legitimation). Detta för att undvika en förvirring när andra delar av kommunen (t.ex. Socialtjänsten) jobbar med Sambis tillitsramverk. Förutsättningarna för arbetet är:

- E-legitimationsnämndens tillitsramverk är den Svenska normen som även Skolfederation ska följa. De befinner sig nu i slutfasen av sitt arbete med att fastställa sitt ramverk och sin granskningsmall.
- Det har framförts från flera Skolhuvudmän att det är ett förstort steg att uppfylla E-legitimationsnämndens tillitsramverks (LoA2 och uppåt).

Vi arbetar därför utefter att:

- Vi ska gå igenom och se vad som behöver göras för att anpassa Skolfederation tillitsramverk till E-legitimationsnämndens tillitsramverk för LoA2 (eller LoA3). Fredrik Ljunggren, konsult från Kirei, återkommer med en rapport. Detta tillitsramverk ska dock anses som ett mål för skolan att jobba mot.
- Baserat på E-legitimationsnämndens LoA2-tillitsramverket tar vi även fram ett förslag på en ”LoA Skolfederation 2013” (där bl.a. kraven på LAS lindras). Det som blir kvar ska både uppfylla Datainspektionens krav på personalens hantering av känsliga personuppgifter och vara ett gott steg på vägen mot LoA2.

Arbetet bedrivs av Staffan Hagnell, .SE, Fredrik Ljunggren, Kirei, och Lennart Henriksson, Sundsvalls Kommun.

### 2.2 Fortsatt arbete

Arbetet fortsätter enligt riktlinjerna ovan. Ett förslag till förenklat tillitsramverk ”LoA Skolfederation 2013” skall tas fram och presenteras till nästa möte.

## 3 Hantering och signalering av den nya kravnivån

### 3.1 Underlag utsänd innan mötet

Det pågår en revidering av Skolfederations avtalsbilaga *Bilaga 2 - Tekniska krav*. I det nya förslaget finns texten nedan. Synpunkter på texten? Vilka ytterligare specifikationer behöver tas fram?

Utdrag ur *Bilaga 2 - Tekniska krav*:

**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 att för Användaren enbart presentera de Intygsutgivare 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*[1]. Attributen för Tillitsnivå presenteras i enlighet med *SAML V2.0 Identity Assurance Profiles*[2] och har följande benämning:

- http://id.skolfederation.se/loa/bas
- http://id.skolfederation.se/loa/sf2013
- http://id.skolfederation.se/loa/loa2

1 http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf
2 http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-01.pdf

- 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 autentiseringsmetoder med olika Tillitsnivåer. Utbytet av information sker inom ramen för *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*[3]. 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:

- http://id.skolfederation.se/loa/bas
- http://id.skolfederation.se/loa/sf2013
- 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.

## 3.2 Diskussion och fortsatt arbete

AP: Kan Skolfederation sätta upp en test IdP som har möjlighet att signalera de olika tillitsnivåerna?

Fråga: Kan man tänka sig en striktare namnsättning, där SP:n algoritmiskt kan utläsa rangordningen mellan de fyra tillitsnivåerna?

Diskussion: Helst inte blanda in LoA i namnet för de två lägre nivåerna, då de inte korresponderar mot någon internationell vädertagen LoA-nivå. Det riskerar då att leda till långa LoA-diskussioner.

Fråga: Vad betyder namnet **sf2013**, dvs den tillitsnivå som är tänkt att uppfylla Datainspektionens krav för personalens som hantering av känsliga personuppgifter och samtidigt vara ett gott steg på vägen mot LoA2?

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

Svar: Namnet är inte tänkt att betyda något speciellt. Om någon insisterar på ett annat namn, så går det bra att höra av sig till Staffan Hagnell.

## 4 Övriga frågor

Fråga 1: Klargör ansvarsfördelningen för hantering av olika LoA-nivåer och då speciellt vilket ansvar har tjänsteleverantören?

Diskussion: Tjänsteleverantörens ansvar är att konfigurera upp tjänsten så att den endast betjänar anrop med rätt LoA-nivå (i Identifieringssvaret). Det är personuppgiftsansvarig som anger vilken tillitsnivå som krävas. För att underlätta för personuppgiftsansvarig definierar Federationsoperatören upp lämpliga LoA-nivåer för Skolfederation. Att använda dessa är dock fortsatt frivilligt för personuppgiftsansvarig.

Fråga 2: Kommer Skolhuvudmännen själva att vara aktuella som utfärdare av e-legitimationer eller kan vi förutsätta att de kommer de förse sin personal med e-legitimation från externa leverantörer? Orsaken till frågan är föratt avgöra hur rimligt det är att hantera granskning av utfärdare av e-legitimationer separat från övrig tillitsgranskning och till och med hänvisa till E-legitimationsnämndens granskning av e-legitimationer.

Diskussion: På sikt kan det vara rimligt att anta att alla Skolhuvudmän kommer att köpa tjänsten utfärdare av e-legitimation.

Fråga 3: Kan Skolfederation hjälpa till med att ta fram mallar för personuppgiftsbiträdesavtal? En första sådan mall efterlystes av Lennart Henriksson för att skriva med Studentlitteratur och Gleerups avseende digitala läromedel.

AP: Staffan Hagnell undersöker vad som finns och möjligheterna för .SE att ta fram sådana mallar.

## 5 Nästa möte

Onsdagen 29 januari 2014, kl 13.00.
Telefon: 08—999212, möteskod 322134