Minnesanteckningar Arbetsgrupp Kontosynk

När: 10 oktober 2021 13:00 – 14:00

Uppdragspunkter

AP	Vad	Tid

Deltagare:
Andreas Galistel, Läromedia
Aras Kazemi, Skolverket
Edin Nuhic, Skolverket
Erik Bäckström, Liver
Hailemichael Nigatu, Skolverket
Hans Ekdahl, Gleerups
Henrik Stendahl, Studentlitteratur
Joe Siltberg, Sambruk
Johan Kronander, Pulsen
Magnus Höglund, Alléskolan
Mats Pålsson, Markaryd
Mattias Hyll, Skolverket
Palle Girgensohn, Pingpong
Rasmus Larsson, Internetstiftelsen
Staffan Hagnell, Internetstiftelsen
Stefan Halén, Internetstiftelsen
Ulrika Ahlgren, Internetstiftelsen
Åsa Jernberg, Internetstiftelsen

1. Uppdatering från federationsoperatör

- 11 metadataentiteter (för 11 medlemmar) i produktionsmiljön
- 17 metadataentiteter i Trialmiljön.
- Förändring: Införande av metadatascope i Kontosynk – runt årsskiftet
    - Angivet metadatascope i organisations SAML-metadata flyttas över automatiskt till Kontosynkentitet(er).

2. Reflektioner efter seminarium 29/9 – Provisionering av skolans information

   Se presentation för ett urval av utvärderingssvar.

   Reflektioner från gruppen:
    - Kan vara begränsande att bara tala om provisionering. SS12000 täcker in mer yta än så. Skolverkets roll är att tillhandahålla digitala motorvägar. Där är

provisionering en del, men sedan finns andra system och processer som bör stödjas. Helheten. Kan man hålla provisioneringsdiskussioner skiljt från standarddiskussionerna?

- Bra seminarium – förtydligande att det finns lösningar för SS12000:2020. Rättelse att argumentation vid seminariet handlade just om för läromedel, inte andra system.
    1. En reflektion är att det finns en tröghet i förändringen där ute. Man nöjer sig med det som fungerar och stannar där.
- Vi kan behöver kommunicera med skolhuvudmän på olika sätt. Ett mer lekmannamässigt sätt för att nå ut till verksamhetspersoner, och ett tekniskt sätt för de redan inskolade teknikerna. Identifiera behovet, sedan se vilken lösning som passar.

3. Diskussionspunkt: Säkerhetslösning/API'er för Skolverkets lösning (Aras Kazemi, Skolverket)

   Med anledning av ett inlägg i Nätverk e-ID i Skolan av Joe Siltberg lyfter Aras upp frågan om Skolverkets säkerhetslösning: Vid implementation av FedTLS tidigare fanns det internt motstånd på Skolverket, det behövde genomföras konfigurationer i lastbalanserare för att det skulle fungera. Därefter implementerades i stället en lagerseparerad lösning driftad av SUNET, där initial autentisering sker med FedTLS för att sedan erhålla en Bearer Token som används för auktorisation till provisioneringsservrar. Detta implementerades bland annat för i ramen av SS12000-standarden finns utrymme för Bearer Token.

   Joe menar att de argument som nyttjats tidigare, "krångligt, svårt, långsamt" inte stämmer, och att Skolverket istället bygger en lösning som andra behöver anpassa sig till. De har dessutom löst FedTLS då ticket switchen finns. Kan inte Skolverket dölja sitt interna tokenutbyte utåt och bara ha ett gränssnitt mot skolorna, FedTLS?

   Just nu utreds även hur discovery av provisionerings-URL:er ska genomföras, eftersom dessa inte kan ingå i FedTLS-federation då de ej är en del av FedTLS.

   Hailemichael menar också att inte låsa in sig till FedTLS är också att öppna upp för andra autentiseringslösningar som kan komma. Vid varje anrop behöver inte heller en mTLS-handskakning genomföras.

   Stefan menar att det är en tydlig nedgradering i säkerhet att gå från mTLS till en token. En token ger rättigheter till den som visar den, oavsett autentisering.

4. Status laget runt

   Uteslöts pga. tidsbrist.

5. Nästa möte – förslag måndag 22 november 13:00-14:00