INTERNET STIFTELSEN

Internetstiftelsens Tekniska Federationsforum

Tekniska nyheter och diskussion

28 oktober 2021

Syfte

- Att från federationsoperatörens håll presentera tekniska nyheter avseende Internetstiftelsens federationer
- Att samla in synpunkter och frågor från omvärlden
- Nätverksbyggande

Om ITFF

- Forumet är i form av ett ”öppet hus” med teknisk inriktning
- Ett forum för både Skolfederation och Sambi
- Typiskt ingen fast agenda eller minnesanteckningar
- Alla är välkomna – medlemmar som icke-medlemmar, leverantörer, integratörer, konsulter

Agenda

- Dagens ämne: FedTLS och hur det fungerar i Skolfederation
- Nyheter från federationsoperatören
- Diskussion och frågestund

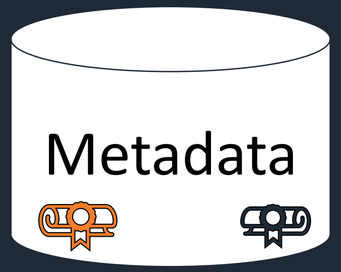

Idag: FedTLS-special!

Federerad TLS

- Ett tunt lager infrastruktur som beskriver hur klienter och servrar kan autentisera varandra på ett federerat vis med den starka autentiseringsmetoden **Mutual TLS Authentication** (ömsesidig TLS-autentisering)
- Finns på GitHub: https://github.com/dotse/tls-fed-auth/
- Skriven av Stefan Halen, Internetstiftelsen, och Jakob Schlyter, Kirei
  - Med input och feedback från bland annat Arbetsgrupp Kontosynk, NLNet (NGI Zero), med flera

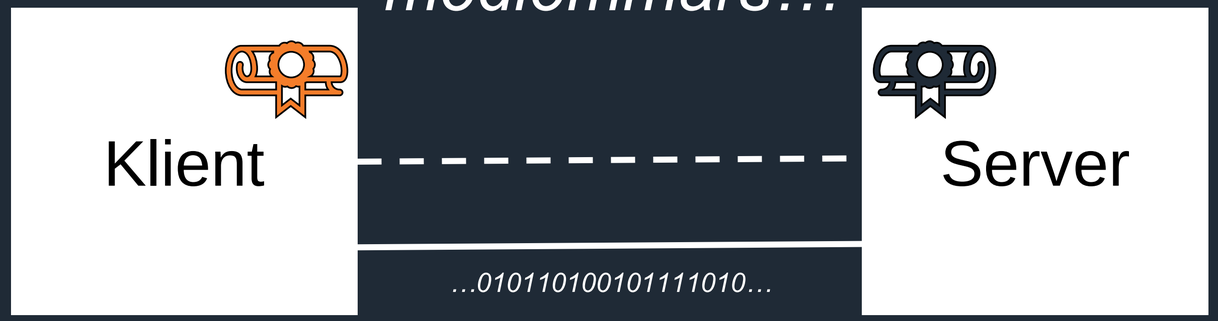
Ömsesidig TLS-autentisering

Federationsoperatören tillhandahåller…



…det vill säga en form av tekniskt medlemsregister…

… som beskriver medlemmars…



… som använder metadatat för att autentisera varandra…

… så att transaktioner kan genomföras över autentiserad och säker kanal

Skolfederation Kontosynk

- Skolfederations tillämpning av FedTLS, produktionssatt november 2019
- Ömsesidig autentisering innan medlemmar i Skolfederation kan skicka data sinsemellan
- Tidigt syfte: säkra provisionering (SS12000 och EGIL)
- Framtida syfte: säkra skolans informationsflöde över organisationsgränser

Skolfederation

Kontosynk
Exempel: provisionering

Federations-metadata Kontosynk

Säkerställda organisationer

Standardiserad informationsmodell

Autentiserade och säkrade kanaler via FedTLS

Skolhuvudman

E-tjänst

E-tjänst

E-tjänst

Standardiserad informationsmodell

Standardiserad informationsmodell

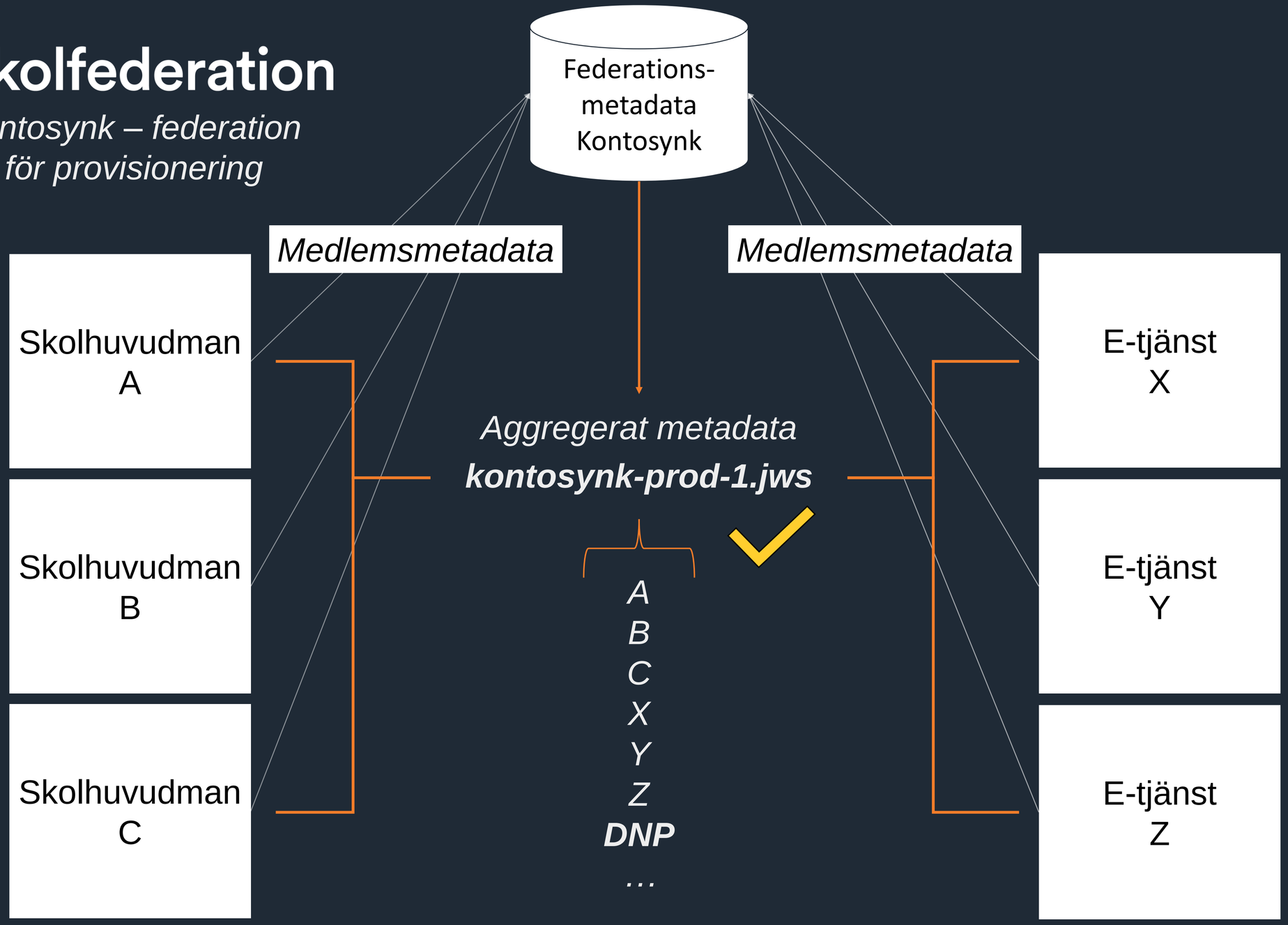
Standardiserad informationsmodell

Standardiserat överföringsgränssnitt

INTERNETSTIFTELSEN

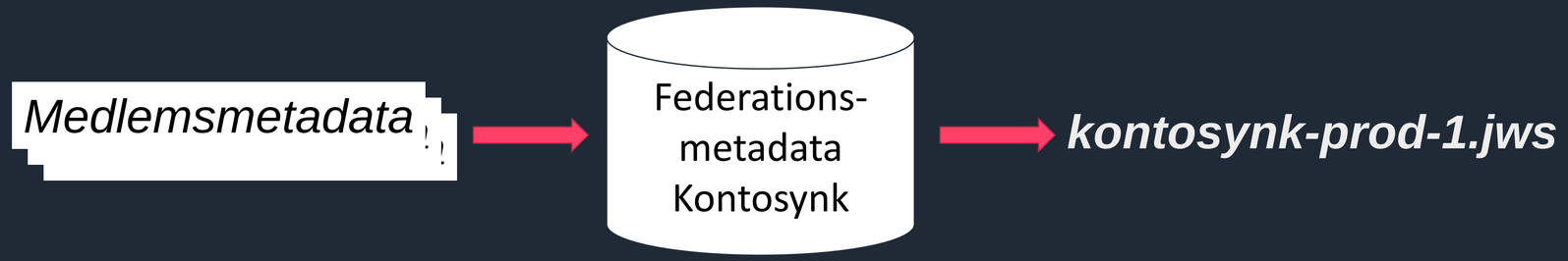
Skolfederation

Kontosynk – federation för provisionering



Skolfederation

Kontosynk – federation för provisionering



- Medlemsmetadata beskriver
  - Ansvarig organisation (inklusive organisationsnummer),
  - Vilken roll organisationen verkar som (Klient eller Server),
  - Utfärdandecertifikat för klient-/servercertifikat och Public Key Pin för identifikation,
  - Vilka tekniska förmågor som servern innehar,
  - Vilka tekniska ändpunkter som kommunikation sker mellan,

- Federationsmetadata Kontosynk beskriver
  - Samtliga medlemmars tekniska metadata, aggregerat och signerat
  - Viss reglering runt hantering av federationsmetadata (ex. giltighetstid och cachetider)

Skolfederation

Kontosynk -
Tekniska Roller

Klient är den part som initierar anslutningen till en **Server**

Dessa roller är inte bundna till om man är **skola** eller **tjänsteleverantör** utan både skolor och leverantörer kan agera Klienter och Servrar beroende på kontext.

Exempel

EGIL-profilen	
Skolhuvudman	**Klient**
Leverantör	**Server**

SS12000:2020	
Skolhuvudman	**Server**
Leverantör	**Klient**

Skolfederation

Kontosynk –
Viktiga metadatakomponenter

Medlemsmetadata

Claim:	Beskrivning:
`entity_id`	Globalt unik identifierare
`clients/servers`	Teknisk roll i federationen
`base_uri`	Base URL för anslutning till server
`pins`	En lista av Public Key Pins, används för anslutning och identifikation av anslutande klient
`issuers`	En lista över godkända certifikatsutfärdare för entiteten

Skolfederation

Kontosynk –
Viktiga metadatakomponenter

Medlemsmetadata

Claim:	Beskrivning:
`tags`	Beskriver serverns funktionalitet (ex. EGIL, SS12000, ...)
`organization`	Namn på organisation som äger entiteten
`organization_id`	Organisationsnummer i format LLÅÅMMDDXXXX där LL är landskod

Skolfederation

Kontosynk –
Exempel metadata

Medlemsmetadata

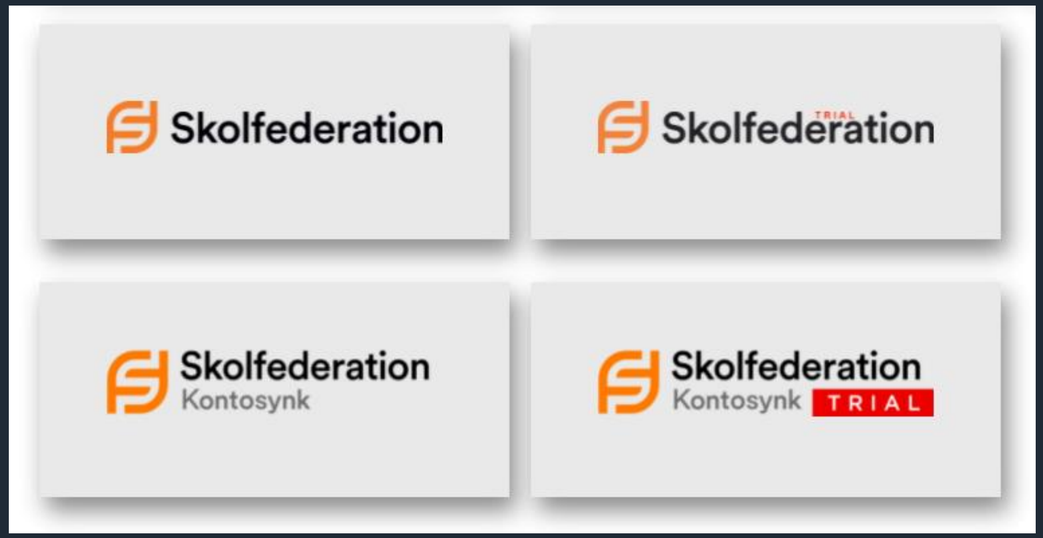
```
{
  "version": "1.0.0",
  "entities": [{
    "entity_id": "https://exempel-skolhuvudman.se",
    "organization": "Exempel Skolhuvudman",
    "organization_id": "SE1122334455",
    "issuers": [{
      "x509certificate": "-----BEGIN CERTIFICATE-----\nMIIDD[…]FPw==\n-----END CERTIFICATE-----" }],
    "clients": [{
      "description": ”EGIL-klient",
      "pins": [{
        ”alg": "sha256",
        ”digest": "+hcmCjJEtLq4BRPhrILyhgn98Lhy6DaWdpmsBAgOLCQ="
      }]
    }]
  }]
}
```

```
"servers": [{
  "description": ”EGIL-server",
  "base_uri": "https://egil.exempeltjanstX.se/",
  "tags": ["egilv1"],
  "pins": [{
    ”alg": "sha256",
    ”digest": "+hcmCjJEtLq4BRPhrILyhgn98Lhy6DaWdpmsBAgOLCQ="
  }]
}]
```

INTERNETSTIFTELSEN

Metadataadministration

- Administration av medlems FedTLS-metadata görs genom Federationsadmin, på motsvarande sätt som görs i SAML-federationen
- Av: Teknisk kontaktperson, eller teknisk agent för medlemmen
- Guide för administration finns här

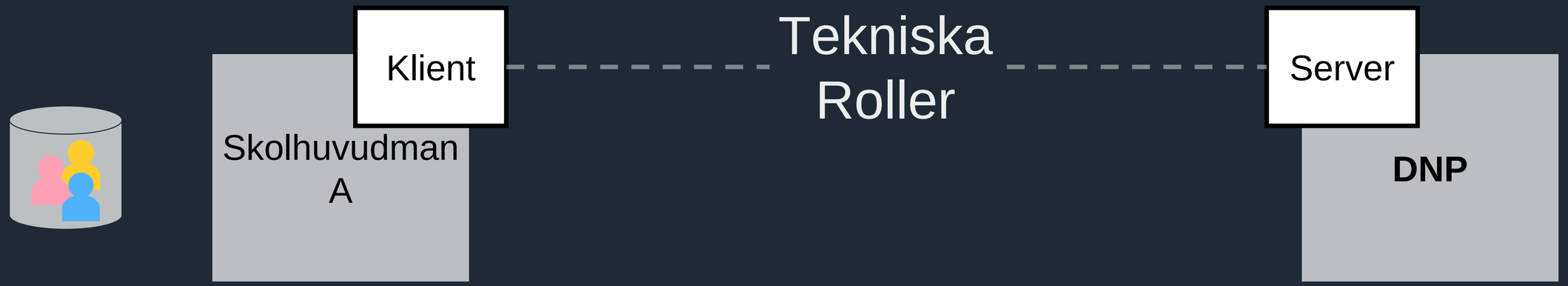


Skolfederation

Anslutning till DNP
genom Federerad TLS

Skolfederation

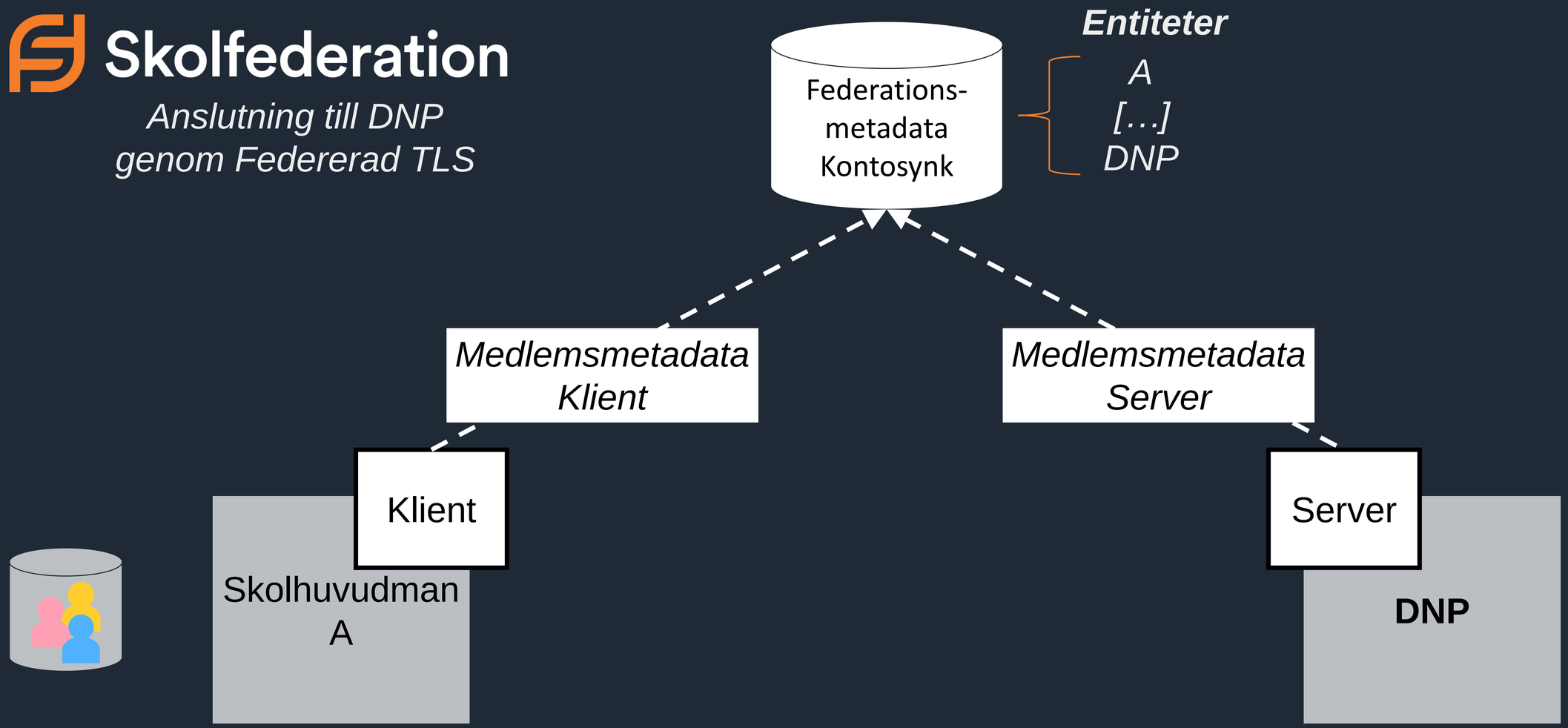
Anslutning till DNP
genom Federerad TLS



**Enligt EGIL-profilen*

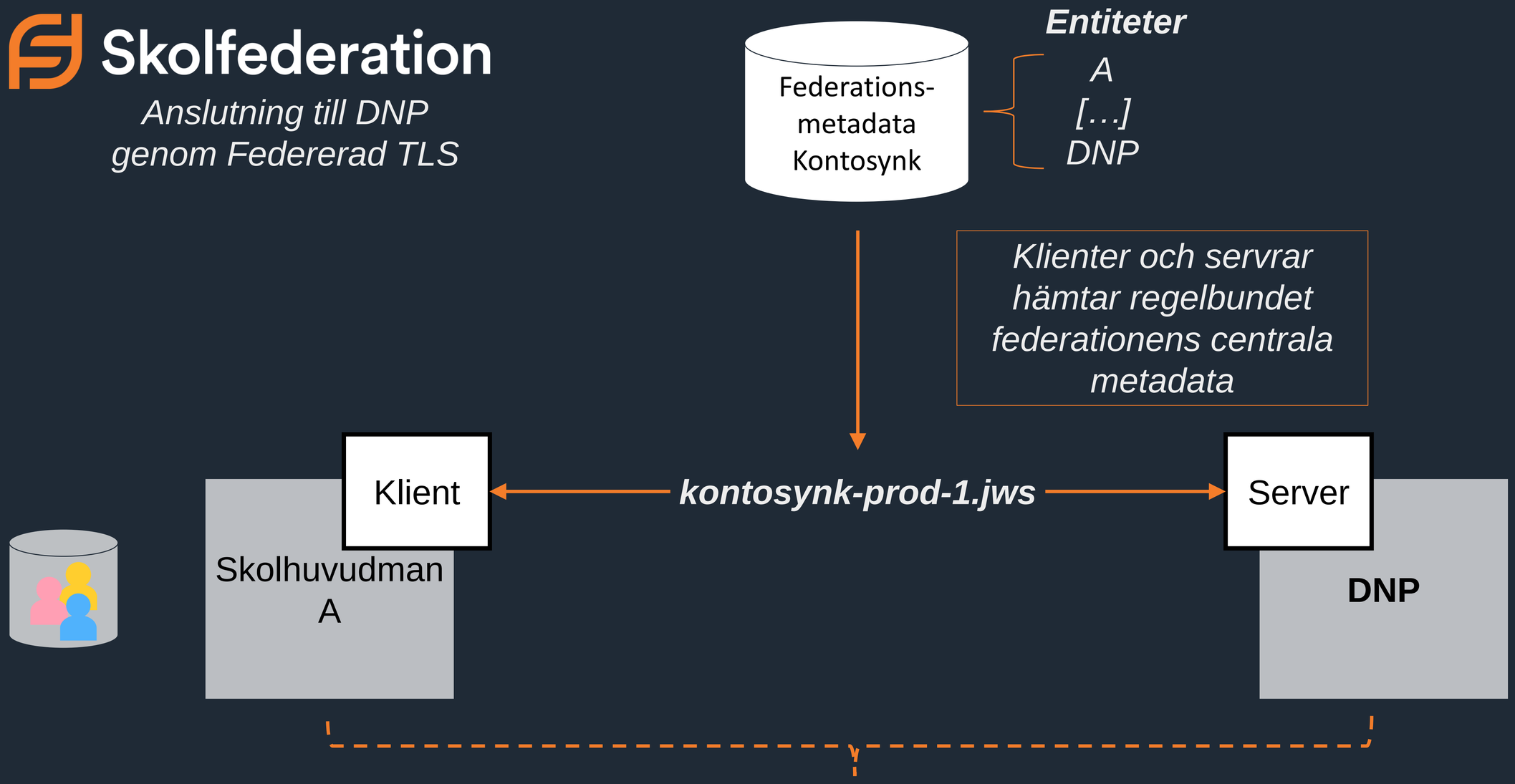
Skolfederation

Anslutning till DNP genom Federerad TLS



Skolfederation

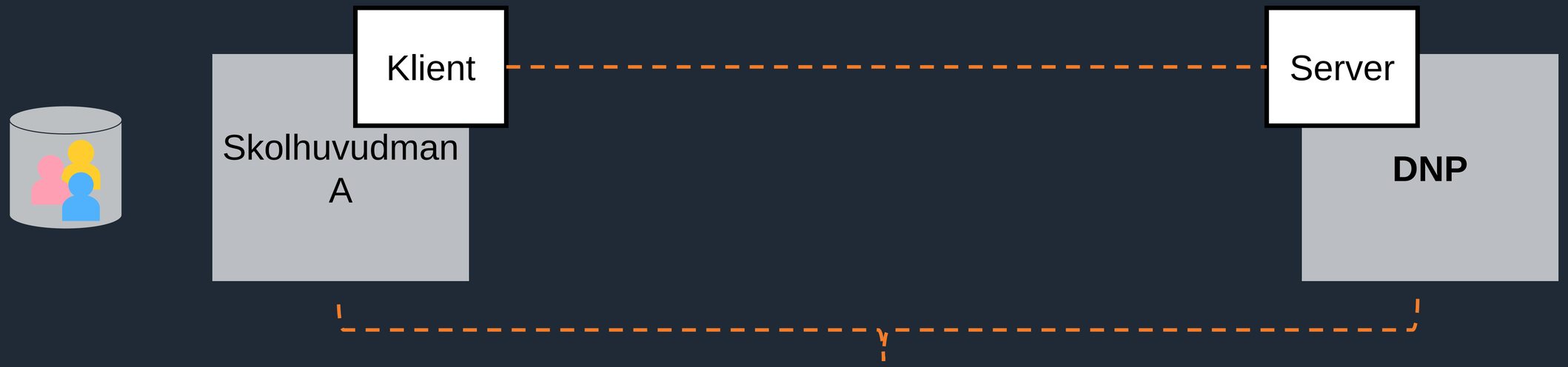
Anslutning till DNP genom Federerad TLS



Skolfederation

Anslutning till DNP genom Federerad TLS

1. Klient anropar Serverns `base_uri` för att initiera TLS-handskakningen
2. Server svarar med Servercertifikat och Klient ombeds presentera sitt Klientcertifikat för Servern



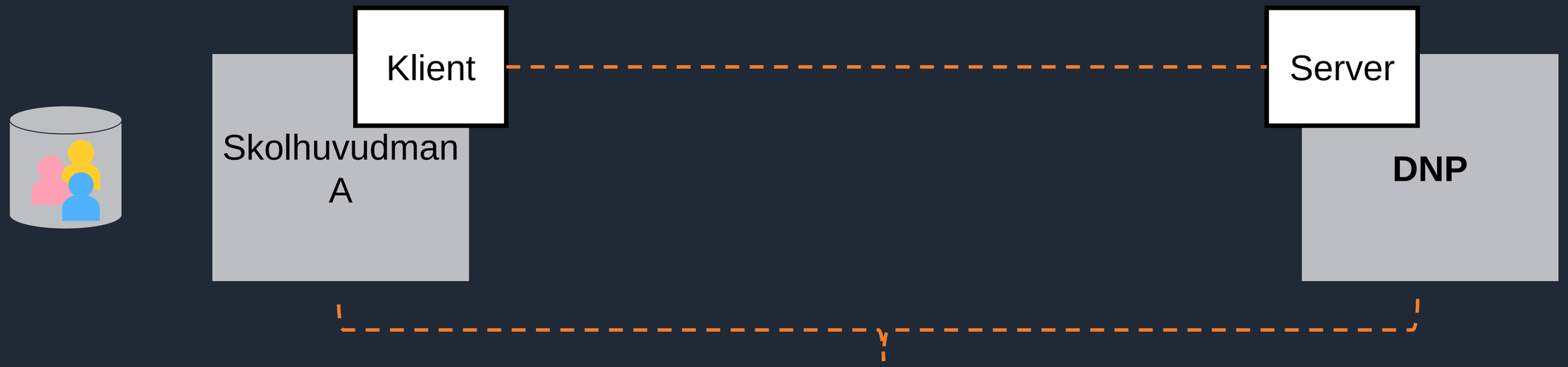
Kännedom om varandras tekniska ändpunkter och certifikat via lokalt cachad kontosynk-prod-1.jws

Skolfederation

Anslutning till DNP genom Federerad TLS

3. Server kontrollerar att Klientens certifikat finns i den lokala databasen över betrodda certifikatsutgivare (baserat på federationens `issuers`)
4. Klient och Server beräknar varandras certifikats Subject Public Key Pin och kontrollerar sedan mot federationens metadata att det stämmer (`pins`)

Servern identifierar även Klienten med hjälp av att hämta tillhörande `entityID` för pin-värdet

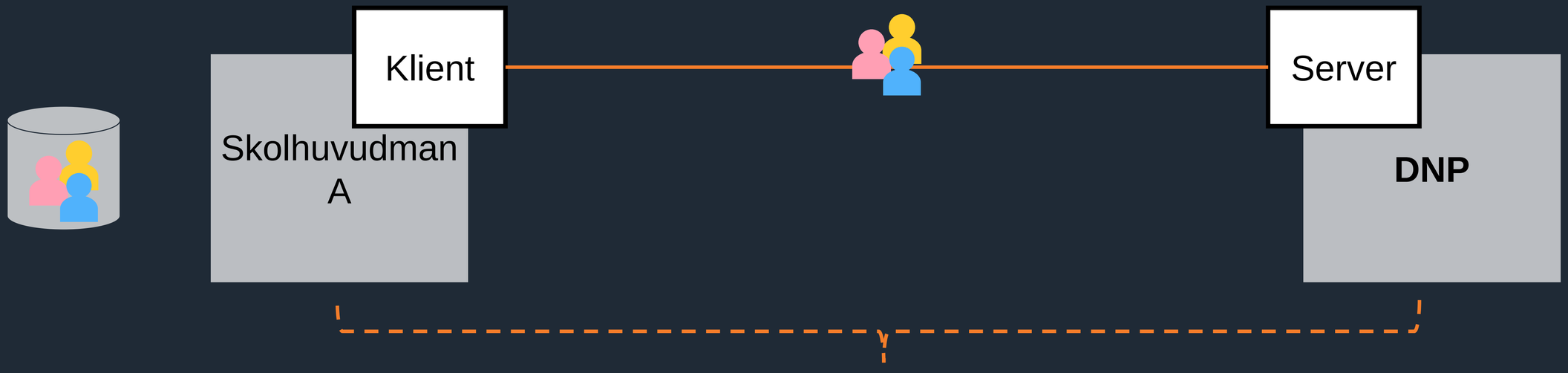


Kännedom om varandras tekniska ändpunkter och certifikat via lokalt cachad kontosynk-prod-1.jws

Skolfederation

Anslutning till DNP genom Federerad TLS

5. Server fattar auktorisationsbeslut baserat på anslutande Klients `entityID`
6. Säker tunnel etablerad - transaktioner kan påbörjas!



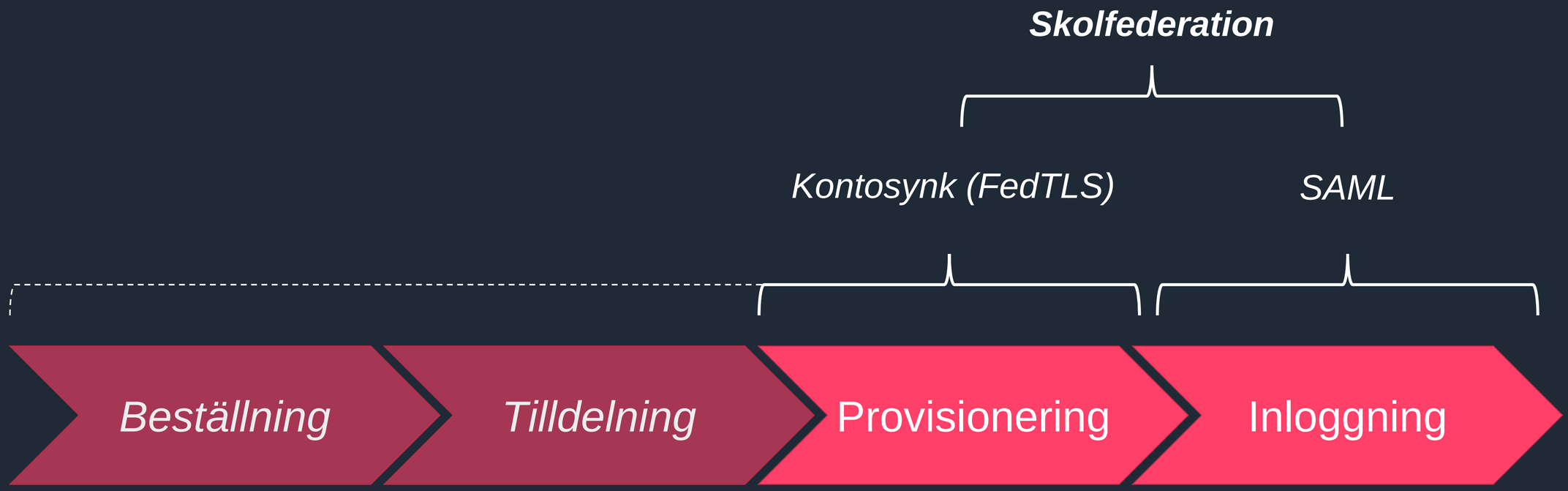
Kännedom om varandras tekniska ändpunkter och certifikat via lokalt cachad kontosynk-prod-1.jws

Tillämpningar inom Kontosynk

- Just nu: EGIL – provisionering enligt EGIL-profilen
- https://sambruk.se/egil-dnp/
- Tänkbara framgent: SS12000:2020, eventuell DNP-specifik profil (i den mån den finns eller kommer), *beställning och leverans* av digitala läromedel…

- *Pågående diskussion: federativt stöd för Beställning och Leverans (BoL) i Skolfederation*

Mer information om BoL finns här (Digitala lärresurser, AG06):
https://www.sis.se/standardutveckling/tksidor/tk400499/sistk450/



Kontosynks tekniska profil

- https://www.skolfederation.se/teknisk-information/kontosynk/teknisk-profil-kontosynk/
- Beskriver utöver FedTLS-standarden hur tillämpning av Kontosynk sker
- **Tags:**
- Just nu: `egilv1`
- Framöver något i stil med:

Namn	Beskrivning	Tillåtna roller	Läs mer

`egilv1`	roller hanterar kommunikation av information enligt EGIL-profilen	Användarorganisation:
		`clients servers`
		Tjänsteleverantör:
		`servers`
			<länk till EGIL-profil/Sambruk>

`ss12k2020v1`	roller hanterar kommunikation av information enligt SS12000:2020	Användarorganisation:
		`clients servers`
		Tjänsteleverantör:
		`clients`
			https://www.sis.se/produkter/informationsteknik-kontorsutrustning/ittillampningar/ittillampningar-inom-utbildning/ss-120002020/

`skvdnpv1`	roller hanterar kommunikation av
	information enligt Skolverkets bestämda delmängd
	av SS12000:2020
		Användarorganisation:
		`clients servers`
		Tjänsteleverantör:
		`clients`
			<länk till Skolverkets beskrivning...>

Skolfederation

Stöd för multipla processer/flöden

Medlemsmetadata

```
{
  "version": "1.0.0",
  "entities": [{
    "entity_id": "https://exempel-skolhuvudman.se",
    "organization": "Exempel Skolhuvudman",

    …

    "clients": [{
      "description": ”EGIL-klient",
        …
    },
    {
      "description": ”BoL-klient",
        …
    }],
    "servers": [{                                  }]
        "description": ”SS12000:2020 server",
        "base_uri": "https://ss12000.skolhuvudman.se/",
        "tags": [”ss12k2020v1"],
  }]
}
```

Fortsatt arbete

- **Arbetsgrupp Kontosynk**: https://www.skolfederation.se/teknisk-information/kontosynk/kontosynk-arbetsgrupp/

- För att Skolfederations medlemmar, leverantörer och andra intressenter ska få möjlighet att följa med och kommentera arbetet med Kontosynk, standardiseringen av Federated TLS Authentication och närliggande ämnen har Internetstiftelsen etablerat en arbetsgrupp för Kontosynk. Arbetsgruppen träffas över videokonferens var sjätte vecka.

- Välkommen att delta! Kontakta mig: rasmus.larsson@internetstiftelsen.se

Namnsättning av ”Kontosynk”

- Kontosynk är ett ganska begränsande namn för att beskriva en federation vars syfte är generellt
- Utredning av namnbyte pågår

Resurser

- Specifikation för FedTLS-autentisering: https://github.com/dotse/tls-fed-auth/

Teknisk profil Kontosynk: https://www.skolfederation.se/teknisk-information/kontosynk/teknisk-profil-kontosynk/

Exempelkod för konsumtion av FedTLS-metadata: https://github.com/Sambruk/federated-tls-auth

Allmän beskrivning av Kontosynk: https://www.skolfederation.se/om/kontosynk/

EGIL-klient: https://github.com/Sambruk/EgilSCIM

Frågor så här långt?

Nyheter från federationsoperatören

Genomförda förändringar

Stabilitet och bugfixar

Diverse stabilitetsförbättrande åtgärder och bugfixar har gjorts för att hålla Federationsadmin i topptrim.

I roadmap

- **Scope i Kontosynkmetadata**

Inkludera Scope i Kontosynkfederationen för att DNP ska kunna koppla ihop inloggande IdP med provisionerande funktion från Kontosynk.

Tidigare förändringar

Alla tidigare förändringar, roadmap, med mera finns publicerad på federationswikin:

https://fedwiki.atlassian.net/wiki/spaces/IFED/pages/856031358/F+rb+ttringar+och+roadmap

Kommande evenemang

Skolfederations seminarieserie

~~2021-09-01 Schrems II-domen, uppföljning~~

~~2021-09-15 Skolans hantering av e-post~~

~~2021-09-29 Provisionering av skolans information~~

~~2021-10-20 Digitala läromedel, uppföljning~~

~~2021-10-27 Förberedelser för digitala nationella prov (DNP), perspektiv: Skolverket och huvudmän~~

2021-11-10 Leverantörernas lösningar för digitala nationella prov (DNP)

2021-11-24 Praktisk hantering av skolans personuppgifter

2021-12-01 Förberedelser för digitala nationella prov (DNP), perspektiv: Skolverket och huvudmän

Var med och påverka i Skolfederation!

Skolfederations referensgrupp - https://www.skolfederation.se/om/referensgruppen/

Medlemskap i referensgruppen är öppet för alla som kan bli medlemmar i Skolfederation, det vill säga användarorganisationer, tjänsteleverantörer och myndigheter.

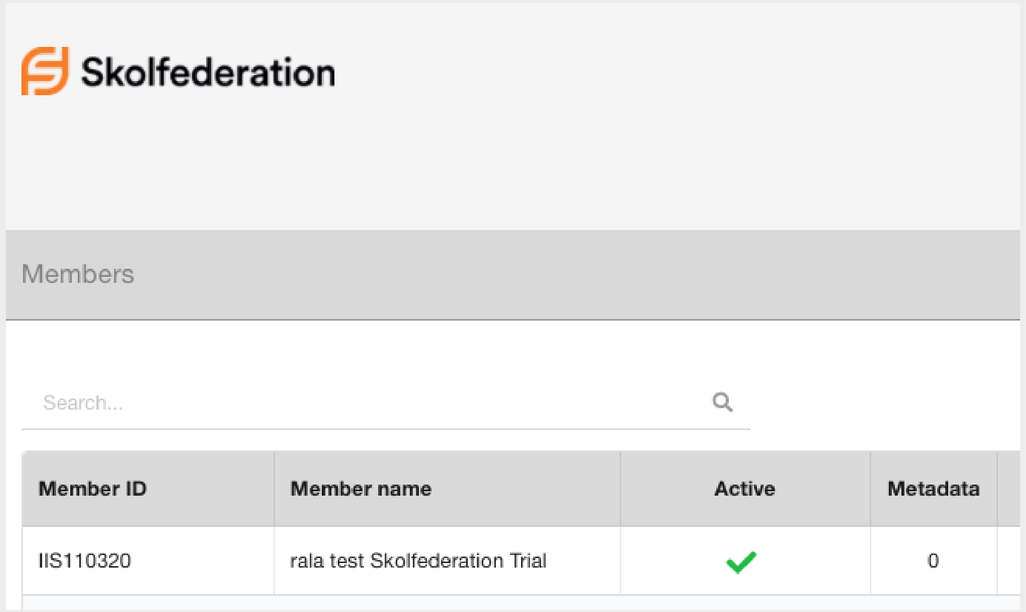
Vill du gå med i referensgruppen, skicka ett mail till info@skolfederation.se.

Två referensgruppsmöten per termin.

Nästa ITFF

13 januari 2021 kl. 13:00-14:30

Förbättringsförslag eller feedback?



Kontakta oss: federationer@internetstiftelsen.se

Diskussion och frågor

För frågor ni önskar ta i mer privata sammanhang så finns vi på info@skolfederation.se samt info@sambi.se respektive.