INTERNET STIFTELSEN

Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkar för ett internet som bidrar positivt till människan och samhället.

INTERNET STIFTELSEN

SSO-länkar och portaler

Informationsmöte med tjänsteleverantörer - 17/5 2024

Johan Sandin johan.sandin@internetstiftelsen.se
Rasmus Larsson rasmus.larsson@internetstiftelsen.se
Robert Rhudin Sundin robert.sundin@internetstiftelsen.se
Stefan Halén stefan.halen@internetstiftelsen.se

E-tikett och formalia

- Stäng av mikrofonen (“mute”) när du inte talar
- Använd Q&A-funktionen eller chatten för att ställa frågor så lyfter vi dessa allt eftersom, eller i frågestunden
- Vi skickar ut presentationen till er i efterhand
- Mötet spelas inte in


Välkomna!

Informationsmöte med tema:
förenkla användares åtkomst till tjänster i federationen

- ”SSO-länkar”
- Portaler
- Och infrastruktur/register i botten

Utvecklingsaktiviteter för förbättringar och ökad funktion i federationernas ekosystem

Våra utvecklingsaktiviteter hittar du på:
wiki.federationer.internetstiftelsen.se/display/IF/Utvecklingsaktiviteter

Och syftet...

- Presentera problemställning och lösningsförslag
- Mottaga synpunkter och feedback från federationens tjänsteleverantörer

Agenda

Nu: Bakgrund och problemställning

Lösningsförslag

Sammanfattning

Öppen diskussion och frågestund

14:55: Mötet avslutas

Obs. primärt på dagens teman.
Frågor relaterade till andra ämnen sparas och besvaras i mån av tid.

Bakgrund och problemställning

Terminologi

- **”SSO-länk”** – populärterm för den länk användaren (ex. elev) använder för att logga in till en tjänsteleverantörs tjänst (SP) federerat via användarens IdP, ofta med SSO, utan anvisning (ex Skolfederations centrala anvisningstjänst).

- **Portal** – en lösning som samlar resurser och länkar till olika tjänster för att möjliggöra enkel åtkomst för användaren, och ofta ”en väg in”. Ibland smarta, ibland mindre smarta.

- **Anvisningstjänst** – en tjänst/funktion där användaren kan hitta sin hemorganisations IdP när SP inte känner till var användaren kommer ifrån. Finns centrala (ex Skolfederations och FIDUS), och egenutvecklade kopplade till var tjänst.

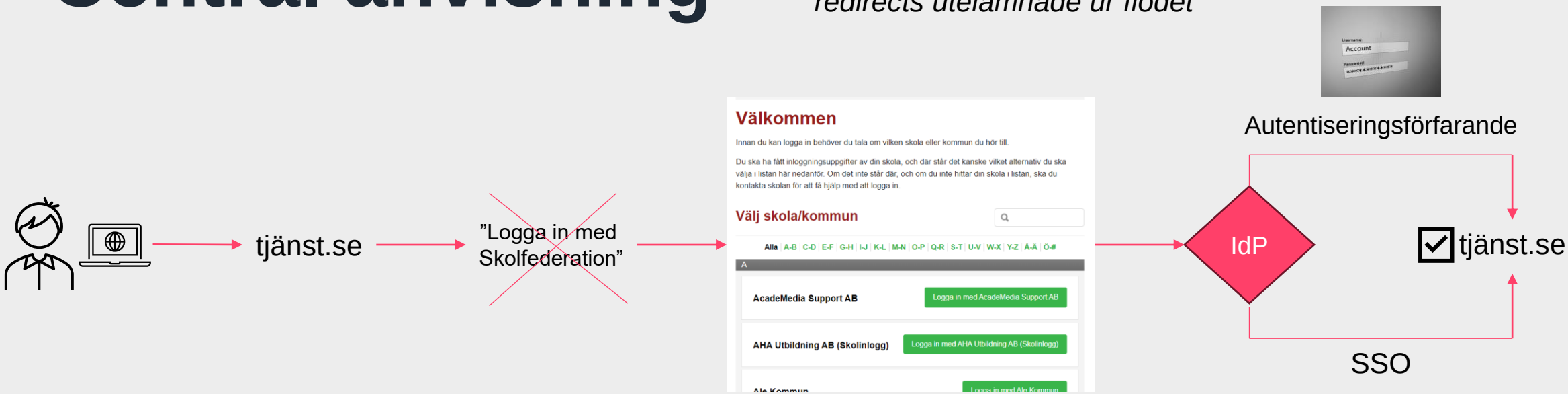
Dagsläget (vår bedömning)

Användare som önskar åtkomst till en tjänst når en tjänst via följande tillvägagångssätt:

- **Central anvisningstjänst**
- **Lokal anvisningstjänst**
- **SSO-länkar av olika former som presenteras på olika sätt i olika lösningar**

Central anvisning

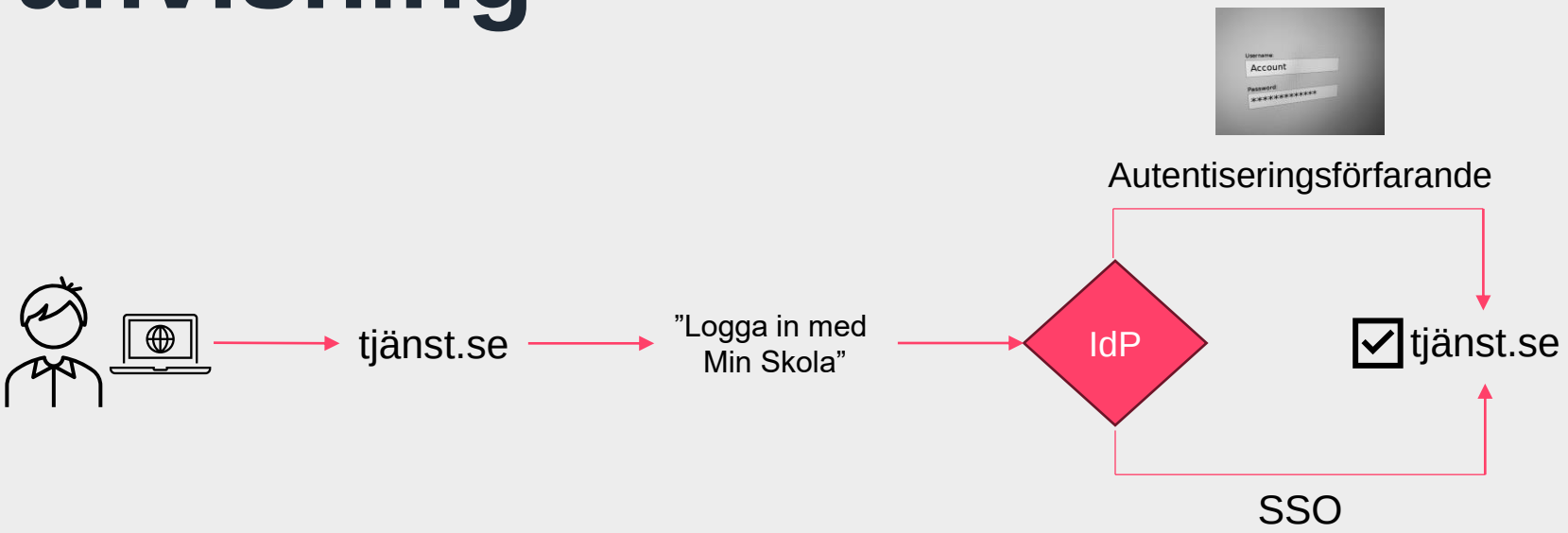
Obs. SP samt tillhörande webbläsar-redirects utelämnade ur flödet



-
Ofta sämre användarupplevelse (extra ”klick”)
Ej anpassningsbar, passar inte tjänst/skolans önskade inloggningsflöde
Innehåller alla IdP’er

+
Backuplösning
Lätt att komma igång (behöver ej utveckla egen)

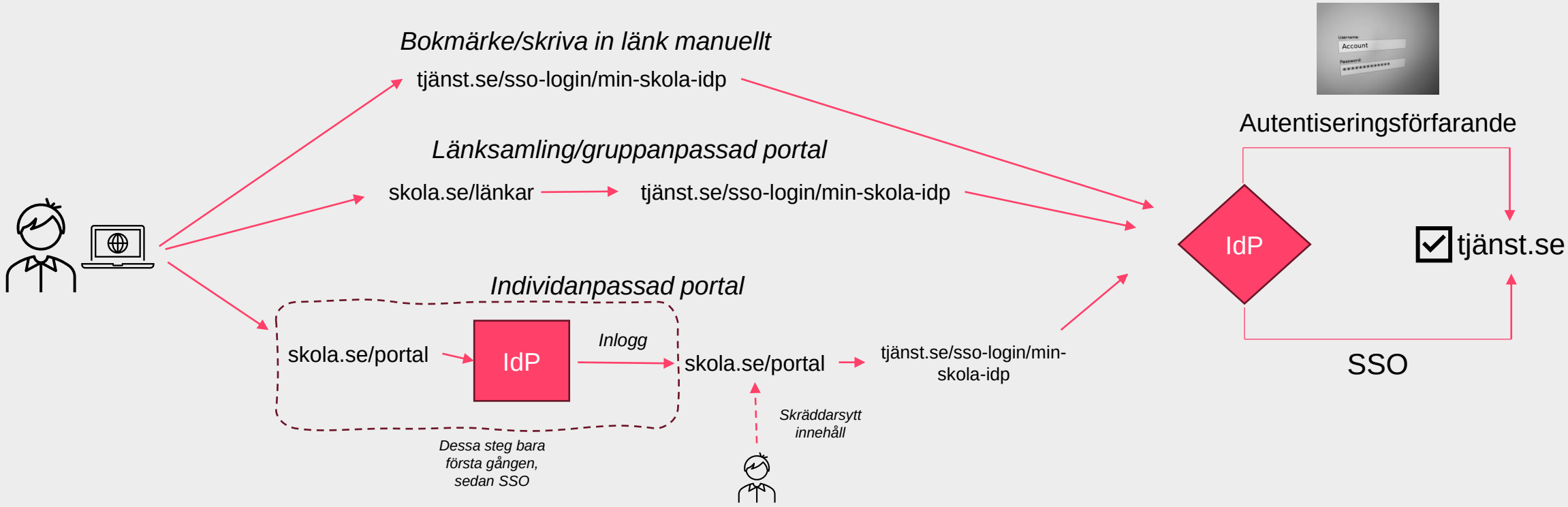
Lokal anvisning



-
Kräver egen utveckling

+
Bra användarupplevelse
Anpassningsbar
Innehåller en tjänsts kunders IdP’er

SSO-länk i variationer



Portal vs. Länksamling

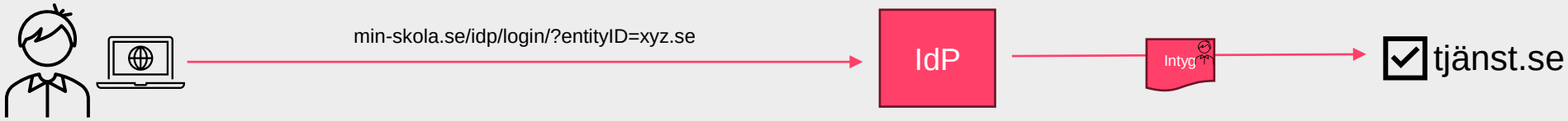
Vad som utgör en portal i detta sammanhang tänker vi är en lösning för att användare ska hitta sina resurser och tjänster på ett smartare sätt än att samla alla länkar på en sida på webben. Exempelvis kan en portal vara kontextanpassad och en portal är användarnära. Den kan också samla annan information av intresse för användaren, och andra stödtjänster.

Helst ska länkarna till tjänsterna inte gå via en anvisningstjänst. En portal är redan en ”omvänd” anvisningstjänst.

Olika typer av SSO-länkar

IdP-initierad inloggning (unsolicited response)

IdP:n skickar ett intyg till tjänsten som tjänsten ej begärde (sk. oombett intyg)



Nackdelar:

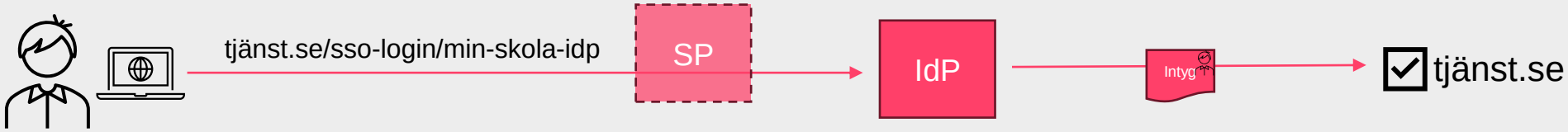
***** Sårbar för man-in-the-middle-attacker – ej rekommenderat

Därför exkluderar vi fortsatt alla tankar om IdP-initierad inloggning i projektet.

Olika typer av SSO-länkar

SP-initierad inloggning

SP:n skickar ett AuthnRequest till IdP, IdP autentiserar användare och skickar ett intyg till tjänsten



Fördelar:

* Säkert, användarvänligt, i bästa fall adminstratörsvänligt

Nackdelar:

* Hur SP-init. SSO-länkar ska formateras är inte standardiserat i federationsvärlden
* Inte alla SP-programvaror stödjer SP-init. SSO-länkar

Olika typer av SSO-länkar

SP-initierad inloggning med parameter som anger IdP entityID
Ex. `tjanst.se/login?idp=[IdP entityID]`

Användarvänligt
Säkert
Kan enkelt automatiseras

Utmaningar:
Ej standardiserat
Olika SP's använder olika parameternamn
(Shib SP: `entityID`, SimpleSAMLPHP: `saml:idp`)

SP-initierad inloggning med egenskriven lösning
Ex. `tjanst.se/login/skolansnamn`, eller `skolansnamn.tjanst.se`, eller innehålla automatgenererade värden som ej kan gissas

Användarvänligt
Säkert

Utmaningar:
Ej standardiserat
Ej gissningsbart
(Antagligen) Ej automatiserbart

Problemställning

Det saknas standardiserade lösningar som hjälper administratörer hos användarorganisationer och tjänsteleverantörer att bygga bra sätt för användare att säkert och smidigt hitta och få åtkomst till de resurser som de ska ha tillgång till, utan att kräva för mycket handjagande och manuell administration

- **Central anvisningstjänst** är en godtagbar backuplösning, men är inte användarvänligt

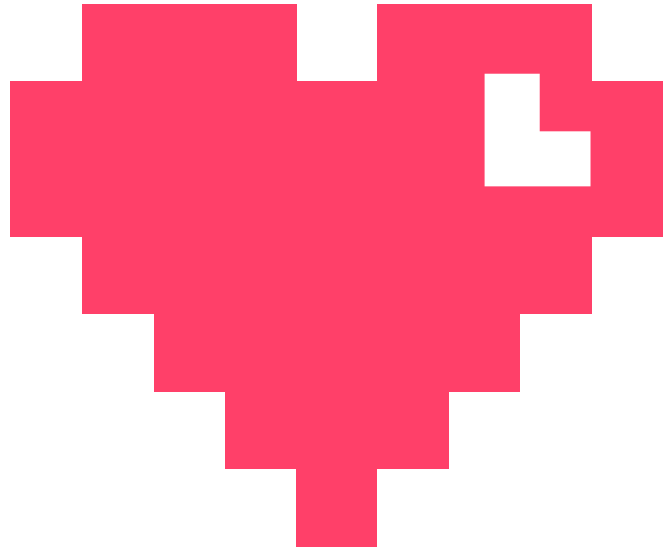
- **Lokala anvisningstjänster** hos tjänsten är bra för åtkomst till tjänst direkt via tjänstens webbsida, men bra anvisningstjänster är tunga att bygga och SAML-metadata innehåller inte utvecklarnära data för att underlätta utvecklingen.

- **SSO-länkar** möjliggör åtkomst via användarorganisationens föredragna lösning (ex portal), men saknar standardisering

- Inte alla skolor har, eller har möjlighet, att bygga **portallösningar** av resursmässiga anledningar, och kan inte utnyttja fulla potentialen i en SSO-lösning

Frågor, kommentarer så långt?

Håller ni med om vår bild eller är den inkomplett/felaktig?



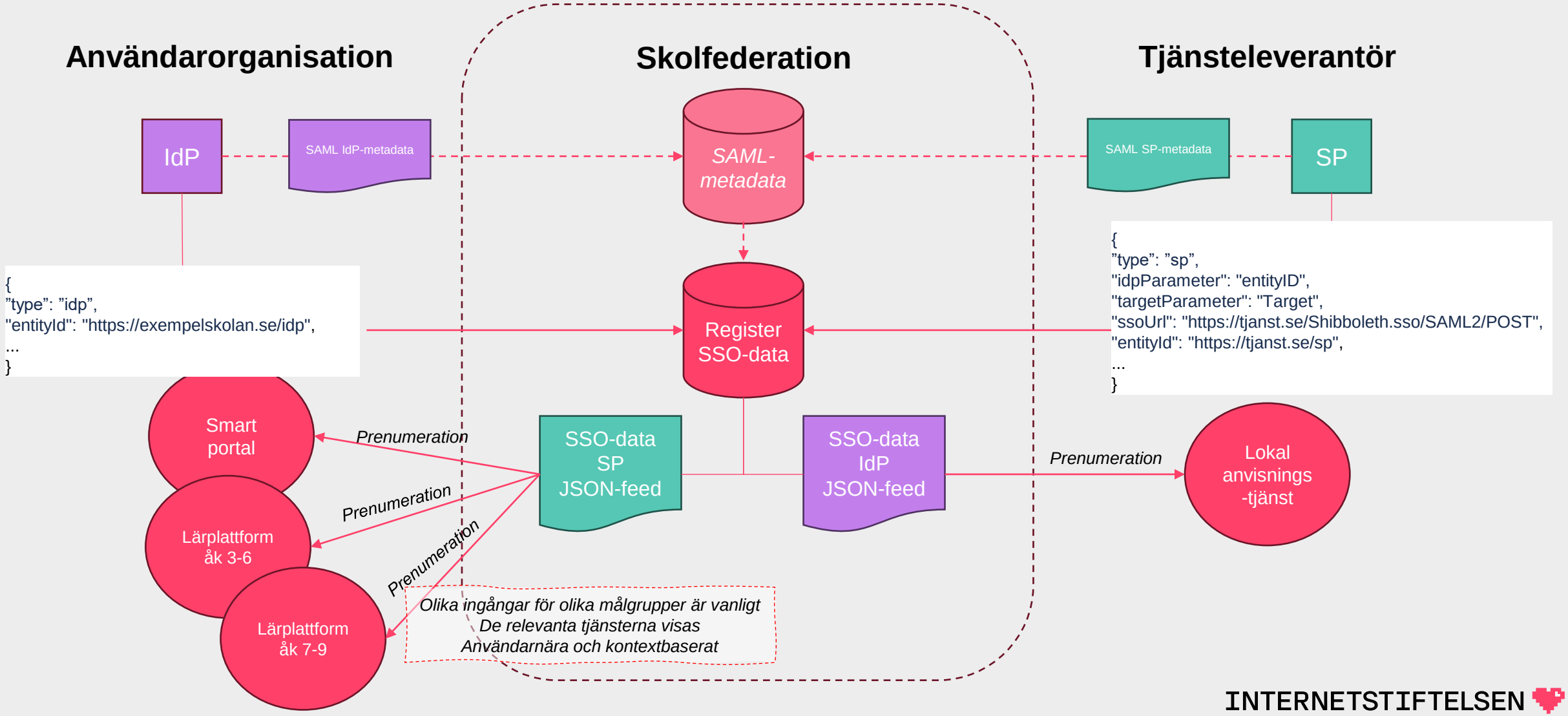
Lösningsförslag

Infrastruktur för SSO-data

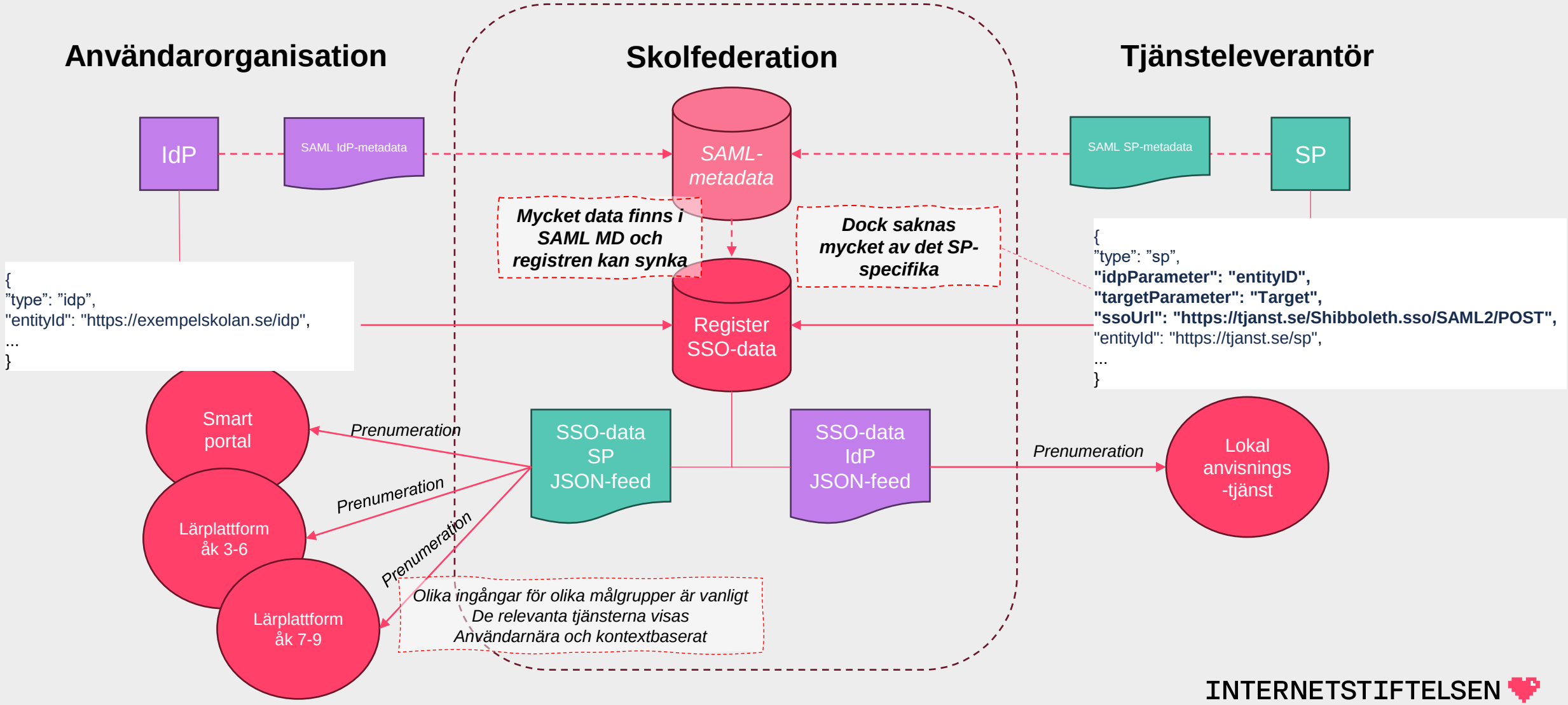
Att ta fram en central infrastruktur/ett register över tjänsters SSO-länkar och annan relevant metadata. Parallellt med detta även ”mer lättläst” metadata om användarorganisationers IdP-lösningar för att förenkla för tjänsteleverantörer. Detta register är separat från SAML-metadata men möjlighet till integration finns.

För att främja användning i federationen tar vi fram tillhörande specifikation/profil för hantering av SSO-länkar i federationen. I sinom tid är målet att den är normativ.

Infrastruktur för SSO-data



Infrastruktur för SSO-data



Exempel på innehåll och struktur i JSON-feed - IdP

Obs. Följande slides är exempel och format, struktur och innehåll är TBD

```
{

            "type": "idp",
            "organizationName": "Exempelkommun",
            "displayName": ”Exempelkommun skola",
            "description": ”Inloggning för elever och personal i Exempelkommun",
            "logo": ”https://exempelkommun.se/logo.png",
            "entityId": "https://exempelkommun.se/idp",
            "software": ”Swedish Cloud Access Manager IdP"

}
```

All denna info kan hämtas från IdP SAML-metadata

Användarorganisationer skulle ej behöva ange ytterligare metadata för SSO-dataström.

Exempel på innehåll och struktur i JSON-feed - SP

Med Shibboleth SP


```
{
        "type": "sp",
        "organizationName": ”Exempel tjänsteleverantör AB",
        "serviceUrl": "https://exempeltjanst.se",
        "displayName": ”Exempeltjänst Lära och Lek",
        "description": ”Lära och Lek för årskurs 1-6",
        "logo": ”https://exempeltjanst.se/logo.png",
        "idpParameter": "entityID",
        "targetParameter": "Target",
        "targetUrl": "",
        "loginUrl": "",
        "ssoUrl": "https://exempeltjanst.se/Shibboleth.sso/SAML2/POST",
        "entityId": "https://exempeltjanst.se/Shibboleth.sso",
        "software": "Shibboleth",
        "spInit": "https://exempeltjanst.se/Shibboleth.sso/Login?",
        "disabled": false

}
```


Fetstilt kan inte hämtas från SP-metadata och kräver därmed att leverantörer tillgodoser feeden med detta extra metadata

Exempel på innehåll och struktur i JSON-feed - SP

Med SimpleSAMLphp

```
{
        "type": "sp",
        "organizationName": ”Exempel tjänsteleverantör AB",
        "serviceUrl": "https://exempeltjanst.se",
        "displayName": ”Exempeltjänst Lära och Lek",
        "description": ”Lära och Lek för årskurs 1-6",
        "logo": ”https://exempeltjanst.se/logo.png",
        "idpParameter": "saml:idp",
        "targetParameter": "ReturnTo”,
        "targetUrl": "",
        "loginUrl": "",
        "ssoUrl": "https://exempeltjanst.se/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp",
        "entityId": "https://exempeltjanst.se/simplesaml/module.php/saml/sp/metadata.php/default-sp",
        "software": ”SimpleSAMLphp",
        "spInit": "https://exempeltjanst.se/simplesaml/module.php/core/as_login.php?AuthId=default-sp&",
        "disabled": false

}
```

name: 'Skolfederation Trial', idpUrl: 'https://samlmd.s3.eu-central-1.amazonaws.com/fedportal/skolfederation-trial/skolfederation-trial-idp-v1.json', spUrl: 'https://samlmd.s3.eu-central-1.amazonaws.com/fedportal/skolfe

Demo-tajm!

Testa själva:

https://md.swefed.se/fedportal/web/index.html?fed=skolfedTrial

JSON-feed SP:
https://samlmd.s3.eu-central-1.amazonaws.com/fedportal/skolfederation-trial/skolfederation-trial-sp-v1.json

JSON-feed IdP:
https://samlmd.s3.eu-central-1.amazonaws.com/fedportal/skolfederation-trial/skolfederation-trial-idp-v1.json

Förutsättningar

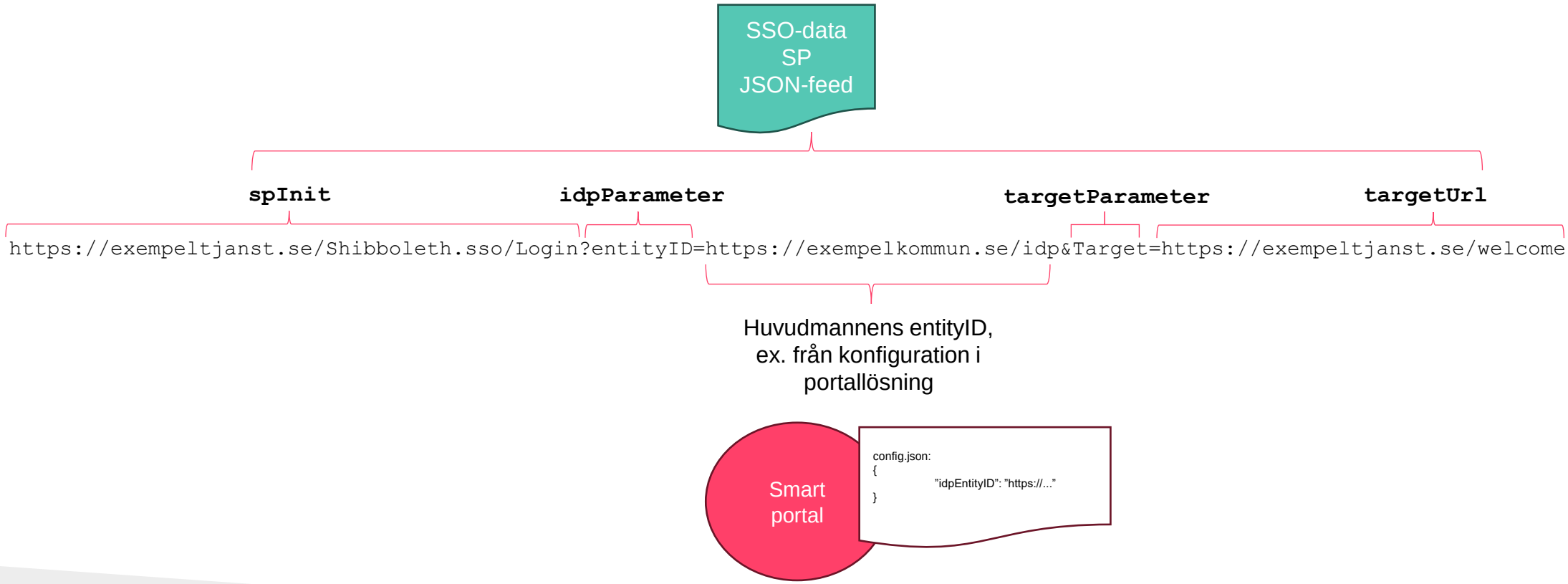
- SP kan hantera SP-initierad inloggning med idpParameter och ev. andra parametrar och anger det via anvisad kanal,

- SP uppdaterar bildelement, beskrivning, och annat relevant MDUI-data i SAML SP-metadata

- IdP uppdaterar bildelement, beskrivning, och annat relevant MDUI-data i SAML IdP-metadata

Tillämpning av SSO-data

Maskinell automatisk uppdatering av SSO-länkar baserat på metadata

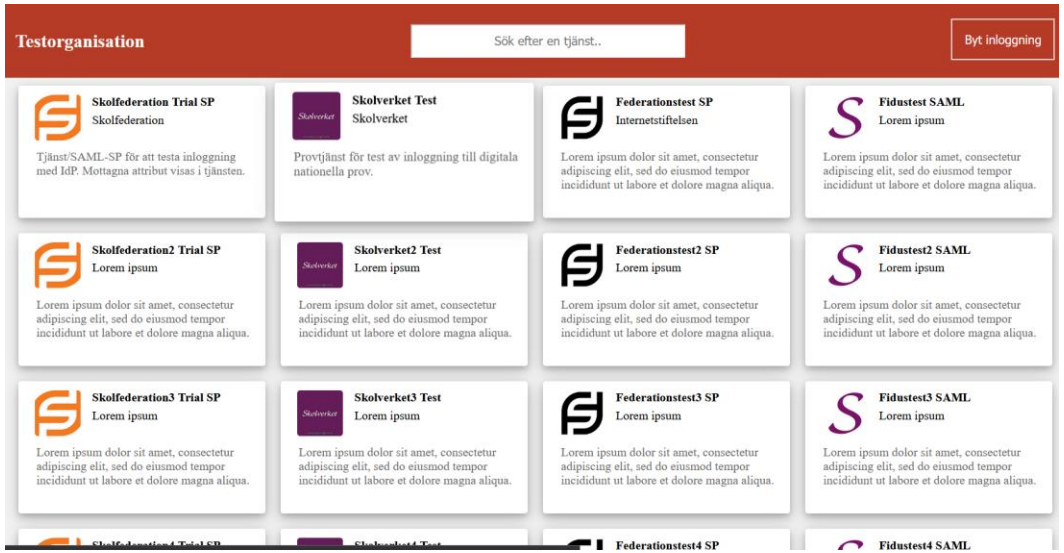


INTERNETSTIFTELSEN

Stödtjänst: portalpaket

Inte alla organisationer har tillgång eller möjlighet att erhålla en portallösning för att förenkla användarens inloggningsflöden.

Som ett stöd till SSO-infrastrukturen tar vi därför fram ett lättviktigt och anpassningsbart ”portalpaket” med inbyggd implementation av SSO-infrastrukturen. Öppen källkod och fri användning.



Stödtjänst: portalpaket

Portalpaketet består av JavaScript, CSS och HTML.

JavaScript:
Lättviktigt script vars övergripande funktioner är att:

- läsa in informationen från JSON-feeder,
- konkatenera parametrar för respektive e-tjänst med parametrar för användarens IdP för att bygga fullständiga SSO-länkar,
- generera HTML för "länkkorten" med bildelement och beskrivning av respektive e-tjänst

HTML:
Mycket lättviktig HTML som utgör grunddokumentet för den HTML som genereras av JavaScriptet.

CSS:
Lättviktig CSS för visuell utformning av HTML-sidan.

Samtliga komponenter utgörs av statiska filer som är anpassningsbara. Krävs ingen CMS eller server för att fungera.

Kan användas tillsammans i sin helhet, eller valda delar tillsammans med egen kod.

Exempel på tillämpningar

Central tjänsteportal

Federationsoperatören tillhandahåller en central tjänsteportal med federationens samtliga tjänster.

Användaren behöver ange vilken organisation (IdP) som länkarna ska baseras på, via val i GUI eller parameter i URL.

Kan fungera som en demonstration av portal med SSO-länkar och ett insteg i portallösningsvärlden, men användarupplevelsen är inte optimal, exempelvis för att alla tjänster i federationen visas upp (motsv. central anvisningstjänst där alla IdP visas upp).

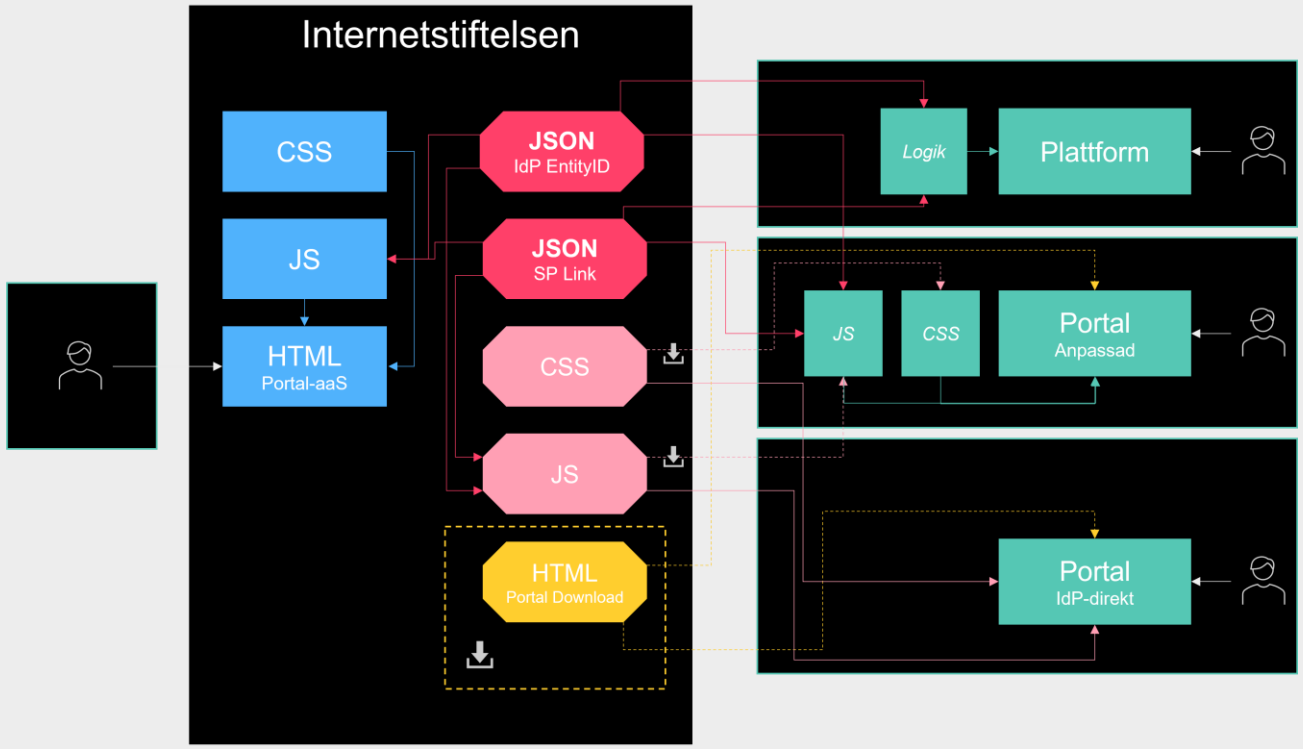
Lokal tjänsteportal

Portalpaketet utnyttjas för att bygga egen lokal portallösning.

Möjliggör lokal konfiguration (ex. standard-IdP och visa enbart relevanta tjänster) och anpassning/branding.

Rekommenderat: om möjligt integrera SSO-data i befintliga portal-, lär-, och andra åtkomstmiljöer som finns i användarens vardag

Överblick över komponenter



Sammanfattning

Vi vill förenkla hanteringen av SSO-länkar för användarorganisation och tjänsteleverantör genom etablering av föreslagen infrastruktur i Skolfederation, tillsammans med portalpaket som stöd.

Denna lösning tänker vi är på plats under HT ’24, och innan den lanseras får tjänsteleverantörer och kommuner testa av och komma med feedback och input om de vill.

Dokumentation och profilering för användning av denna infrastruktur följer.

Sedan behöver den ett bra namn ☺

Finns intresse att delta i projektet och testa av infrastrukturen?

Var med och påverka lösningens utformning!

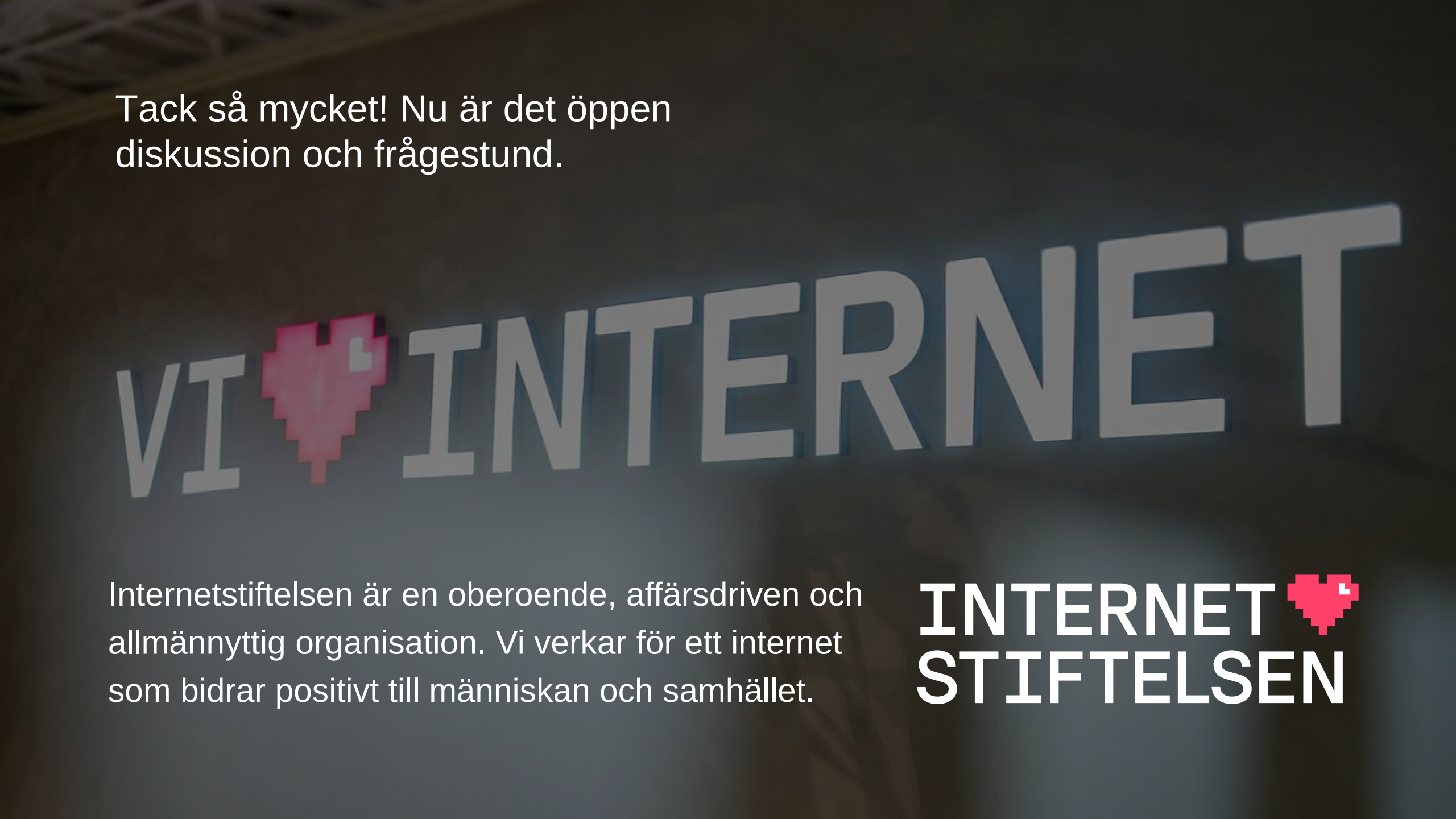
Vi skickar ut ett formulär efter mötet för att samla intresse.

Arbetet samlas på federationens wiki

https://wiki.federationer.internetstiftelsen.se/display/IF/Utvecklingsaktiviteter

Har ni frågor, kontakta info@skolfederation.se.

Tack så mycket! Nu är det öppen diskussion och frågestund.



Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkar för ett internet som bidrar positivt till människan och samhället.

INTERNET STIFTELSEN