SSO-länkar

This information is aimed at Swedish readers. Development items put into production will be documented in English and published in the relevant place in this wiki.

Utvecklingsaktivitet

Kortfattad beskrivning	JSON-feed innehållande data för SP-initierad inloggning med IdP-parameter
Status	UTVECKLING PÅGÅR

Nedanstående beskrivning syftar endast till att ge en översiktlig beskrivning av utvecklingsaktiviteten. Om du är intresserad av mer information, har synpunkter på lösningen eller vill bidra med idéer så kan du kontakta federationsoperatören på info@skolfederation.se eller info@sambi.se.

Bakgrund

En användare behöver en URL för att hitta till respektive tjänst.

I praktiken finns två olika sätt att möjliggöra detta genom en anvisningstjänst eller IdP-initierad session:

- Direktlänkar kan användas genom en IdP-initierad session.
  Från ett säkerhetsperspektiv är inte alltid detta en väg som rekommenderas då det kan utnyttjas med olika tekniker som t.ex "man in the middle" attacker.
- En anvisningstjänst är en funktion som har ett berättigande men är inte alltid önskvärt för att underlätta för en slutanvändare.
  Det kan vara en utmaning för användare att välja rätt IdP utifrån den mängd som presenteras av anvisningstjänsten.

En möjlig utvecklingsfunktionalitet är att använda **SP-initierad session** där:

- Varje URL pekar på SP med anvisning om omdirigering till IdP.
- En unik länk per mjukvara och SP (om förmågan finns) som inkluderar en retur URL till SP efter slutförd autentisering.

Ovanstående metod kallar vi, i denna text, för SSO-länkar.

Utmaning med SSO-länkar

Denna typ av länkar skapas i regel av huvudmannen och presenteras vanligen för användaren i form av en portal eller länkar i någon form av lärmiljö.

För att huvudmannen ska kunna skapa länken behöver den ha kännedom om specifika parametrar för respektive tjänst (förutsatt att tjänsten överhuvudtaget stödjer denna typ av länkar). Eftersom informationen är unik per tjänst och inte finns presenterad i tjänstens metadata så behöver huvudmannen kontakta varje tjänsteleverantör och sedan skapa länkarna manuellt.

Utvecklingsmöjlighet

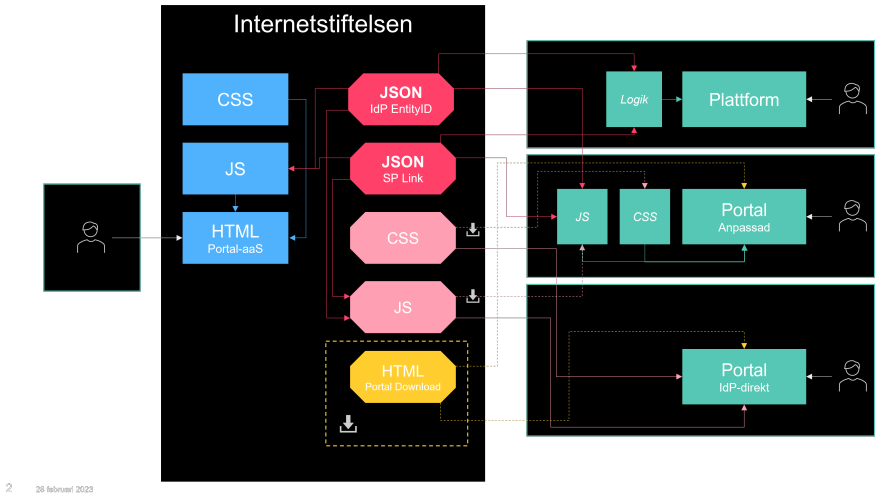
Federationsoperatören samlar in de specifika parametrar som krävs från respektive tjänsteleverantör och publicerar dessa i en JSON-feed. Denna information kan sedan nyttjas av huvudmannen för att automatiskt generera SSO-länkar (informationen kan givetvis användas även för att generera länkar manuellt).

För att underlätta ytterligare så publiceras även en JSON-feed med IdP-data. Denna information är redan tillgänglig för huvudmannen, men genom att publicera den i detta format underlättas automatgenerering av de fullständiga länkarna.

Då denna typ av länkar ofta publiceras för användaren i form av ikoner (tjänstens logotyp), tjänstens namn och en kortfattad beskrivning av tjänsten så kommer även denna information att finnas med i JSON-feeden.

Potentiella tillämpningar

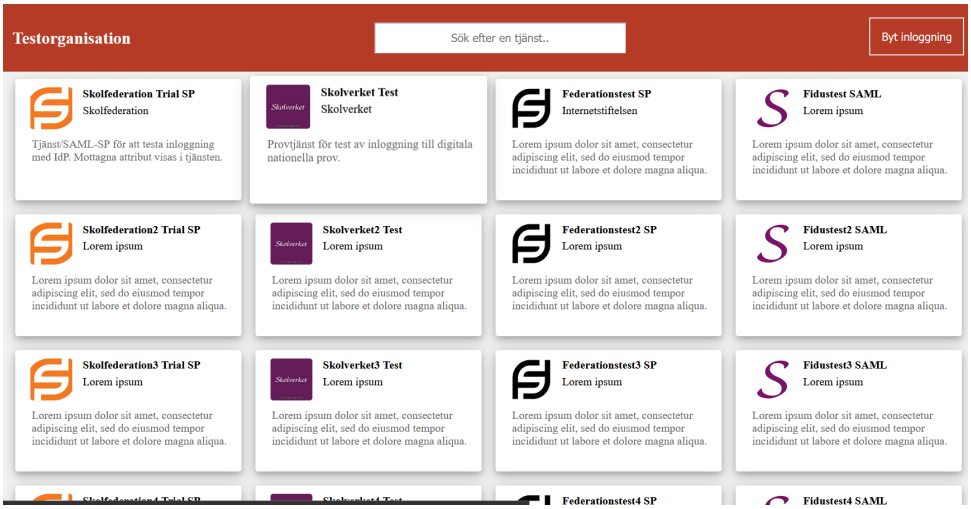
Informationen i JSON-feederna kan tillämpas i många olika lösningar. Nedan presenteras en översiktsbild och några tänkbara tillämpningar.



Bilden ovan illustrerar hur federationsoperatören (Internetstiftelsen) tillhandahåller JSON-feeder, men även en lättviktig portal med federationens samtliga tjänster (en slags omvänd anvisningstjänst). I exemplet tillhandahåller federationsoperatören även JavaScript, HTML och CSS som kan användas för att bygga egna portallösningar.

Bilden visar även hur länkarna kan nyttjas i andra portallösningar och plattformar och kan då, med automatik, anpassas för respektive användare och scenario.

Nedan visas ett exempel på en portal med "dummydata".



Se även den relaterade utvecklingsaktiviteten Tjänsteportal.

Förutsättningar

Kräver att tjänsteleverantörer i federationen har stöd för denna typ av SSO-länkar och försett federationsoperatören med:

- Bildelement MDUI i SAML-metadata
- Description i SAML-metadata
- IdP-parameter och SSO-länk i anvisad kanal

Ytterligare möjligheter

JSON-feeden med IdP-data kan nyttjas av tjänster för att underlätta att bygga en egen anvisningstjänst. Även om många huvudmän skulle välja att nyttja någon form av portallösning så behöver en tjänst kunna hantera användare som accessar tjänsten på annat sätt.

Längre fram kan det bli aktuellt med fler utvecklingsinsatser för att underlätta ytterligare för tjänster att skapa egna, anpassade anvisningstjänster.

Innehåll i JSON-feeder

> ⚠ Detta är under utveckling och formatet på publicerad data kan skilja sig från exemplen nedan.

Ett exempel för en IdP kan se ut som nedan:

```
{
            "type": "idp",
            "organizationName": "Stockholms stad",
            "displayName": "Stockholms stad",
            "description": "",
            "logo": "",
            "entityId": "https://login001.stockholm.se",
            "software": "CASiteMinder"
        }
```

SSO-länkar skiljer sig åt mellan SP-mjukvaror. Ett exempel för en SP som använder **Shibboleth** kan se ut som nedan:

```
{
            "type": "sp",
            "organizationName": "Stockholms universitet",
            "serviceUrl": "https://www.su.se",
            "displayName": "sp-test.it.su.se",
            "description": "Testa attribut-releaser fr\u00e5n IdPer",
            "logo": "",
            "idpParameter": "entityID",
            "targetParameter": "Target",
            "targetUrl": "",
            "loginUrl": "",
            "ssoUrl": "https://sp-test.it.su.se/Shibboleth.sso/SAML2/POST",
            "entityId": "https://sp-test.it.su.se/Shibboleth.sso",
            "software": "Shibboleth",
            "spInit": "https://sp-test.it.su.se/Shibboleth.sso/Login?",
            "disabled": false
}
```

Ett exempel för en SP som använder **SimpleSAML** kan se ut som nedan:

```
{
            "type": "sp",
            "organizationName": "Internetstiftelsen",
            "serviceUrl": "https://Skolfederation.se",
            "displayName": "Skolfederation Trial-SP",
            "description": "",
            "logo": "",
            "idpParameter": "saml:idp",
            "targetParameter": "ReturnTo",
            "targetUrl": "",
            "loginUrl": "",
            "ssoUrl": "https://sp.trial.skolfederation.swefed.se/simplesaml/module.php/saml/sp/saml2-acs.php
/default-sp",
            "entityId": "https://sp.trial.skolfederation.swefed.se/simplesaml/module.php/saml/sp/metadata.php
/default-sp",
            "software": "SimpleSAMLphp",
            "spInit": "https://sp.trial.skolfederation.swefed.se/simplesaml/module.php/core/as_login.php?
AuthId=default-sp&",
            "disabled": false
 }
```

Portal Demo

Länkarna nedan leder till en tidig mockup som visar hur en enkel portal kan genereras med relativt lite kod utifrån data i JSON-feederna. Data i feederna är ren dummydata och koden är inte lämplig att använda i produktion.

https://fedportal.robertsundin.se/

https://fedfeeds.robertsundin.se/sp/json/splink.json