E-hälsomyndighetens säkerhetslösning för Nationell Läkemedelslista

Detaljering av mönster

2021-03-23

Detaljering av mönster

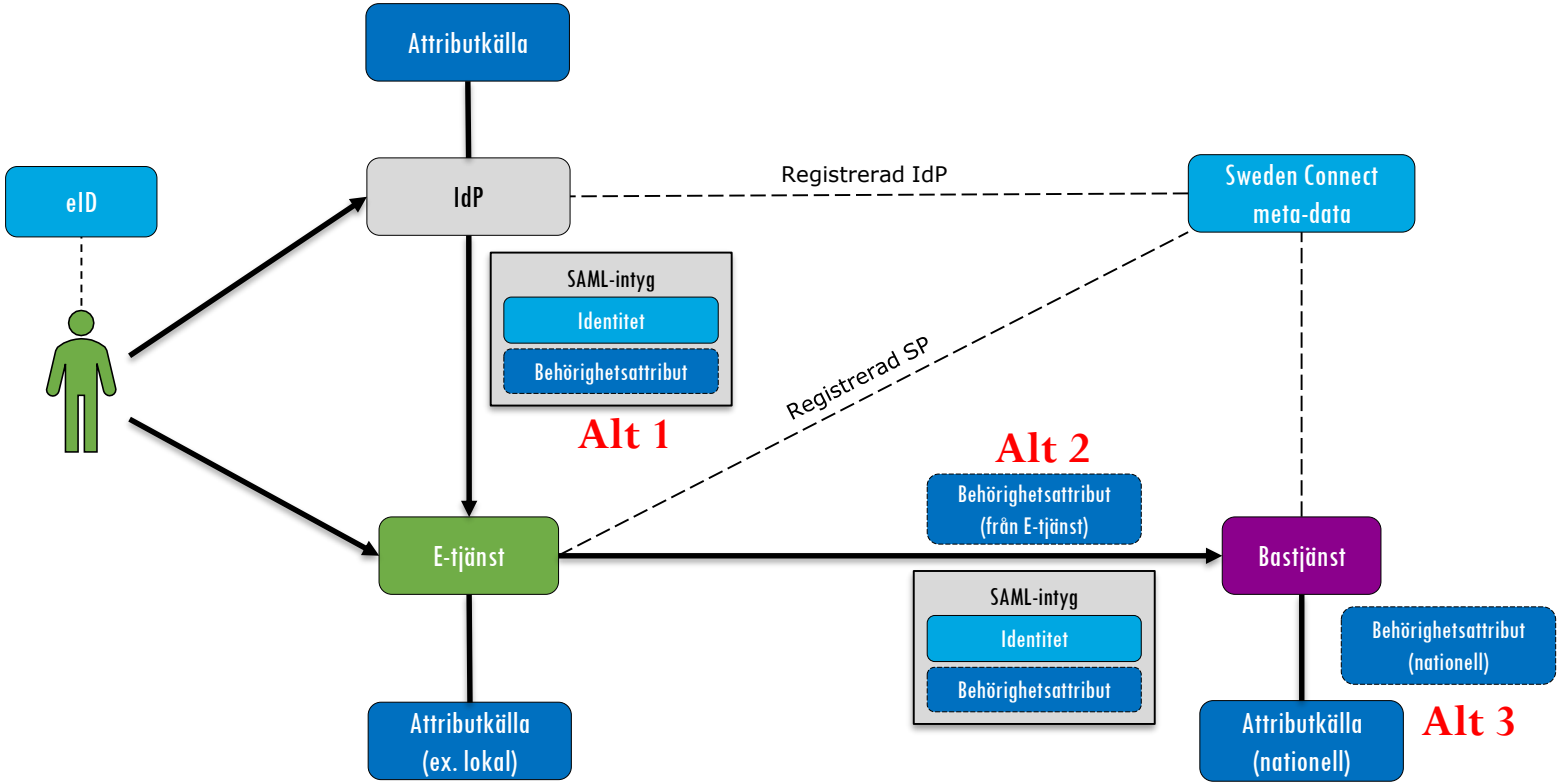
- Snabb återblick alternativ/mönster
- Intygsväxling
- Dekryptering identitetsintyg
- Överföring behörighetsstyrande attribut

Snabb återblick alternativ/mönster

Snabb återblick alternativ/mönster

- **Alt 1: Attribut som en del av identitet-/åtkomstintyget**
  - Behörighetsattribut i intyget (som idag)
- **Alt 2: Separation mellan identitet och behörighetsattribut**
  - E-tjänst förmedlar attribut vid sidan av intyget.
- **Alt 3: Nationella attributkällor för behörighetsattribut**
  - Färre attribut behöver förmedlas. Uppslag/kompletteringar sker hos tjänsteproducenten utifrån behov och möjlighet till.

E-tjänst till Bastjänst (kombination)



eHälsomyndigheten

Intygsväxling

Intygsväxling

- Intygsväxling kommer bli mer aktuell då Sweden Connect har kortare livslängd på utställda identitetsintyg.
- Växling sker från identitetsintyg (SAML) till åtkomstintyg (Oauth2) och förnyelseintyg.
  - Alternativt genom förnyelseintyget då endast nytt åtkomstintyg utfärdas.
- Växling sker utifrån RFC 7522 med anpassningar

RFC 7522 Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants

Intygsväxlingar - anpassningar

- Endast stöd för flödet Assertion Flow / Implicit Flow.
- Inget stöd för revokering av intyg (access & refresh).
- Identifiering av aktörssystem med hjälp av Client identifier och client secret.
  - Client-id är att likställa med EntityId-från SAML-metadata för SP.
  - Inget stöd för identifiering av aktörssystem med SAML-intyg (client_assertion)

Intygsväxlingar - anpassningar

- Endast klienter av typen Confidential kommer att stödjas då dessa ska kunna hantera client secret på ett adekvat sätt.
- Åtkomstintyget är krypterar och därmed inte läsbar för annan part än eHälsomyndigheten.
- Inget stöd för introspection
- Inget stöd för "prompt", dvs påkalla slutanvändarens uppmärksamhet.
- Endast stöd för HTTP Basic som autentiseringsmetod för klienter. [RFC 6749, 2.3.1]

Intygsväxling – Exempel på anrop

```
POST /token HTTP/1.1
Host: as.receptpartner.se
Authorization: Basic <CLIENT_ID>:<CLIENT_SECRET>
Content-Type: application/x-www-form-urlencoded

grant_type=urn:ietf:params:oauth:grant-type:saml2-bearer&assertion=<SAML_ASSERTION>
```

```
grant_type=refresh_token&refresh_token=<REFRESH_TOKEN>
```

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{
    ”access_token”:”<JWE-TOKEN>",
    ”token_type”:"Bearer",
    ”expires_in”:3600,
    ”refresh”:<REFRESH_TOKEN>
}
```

OBS! Bara vid initial växling från SAML

Information om intygsväxling

Handboken

Teknisk information

Anropsinformation 17.1, kap 3

Dekryptering identitetsintyg

Dekryptering identitetsintyg

- SAML-response som skickas från IdP till SP inom Sweden Connect är krypterat.
- SP/E-tjänst behöver dekryptera meddelandet och extrahera SAML-assertion från SAML-response och intygspropagera SAML-assertion till E-hälsomyndigheten vid anrop eller intygsväxling.
- Viktigt är att SAML-assertion är signerad så att den kan verifieras fristående från SAML-response. (->)

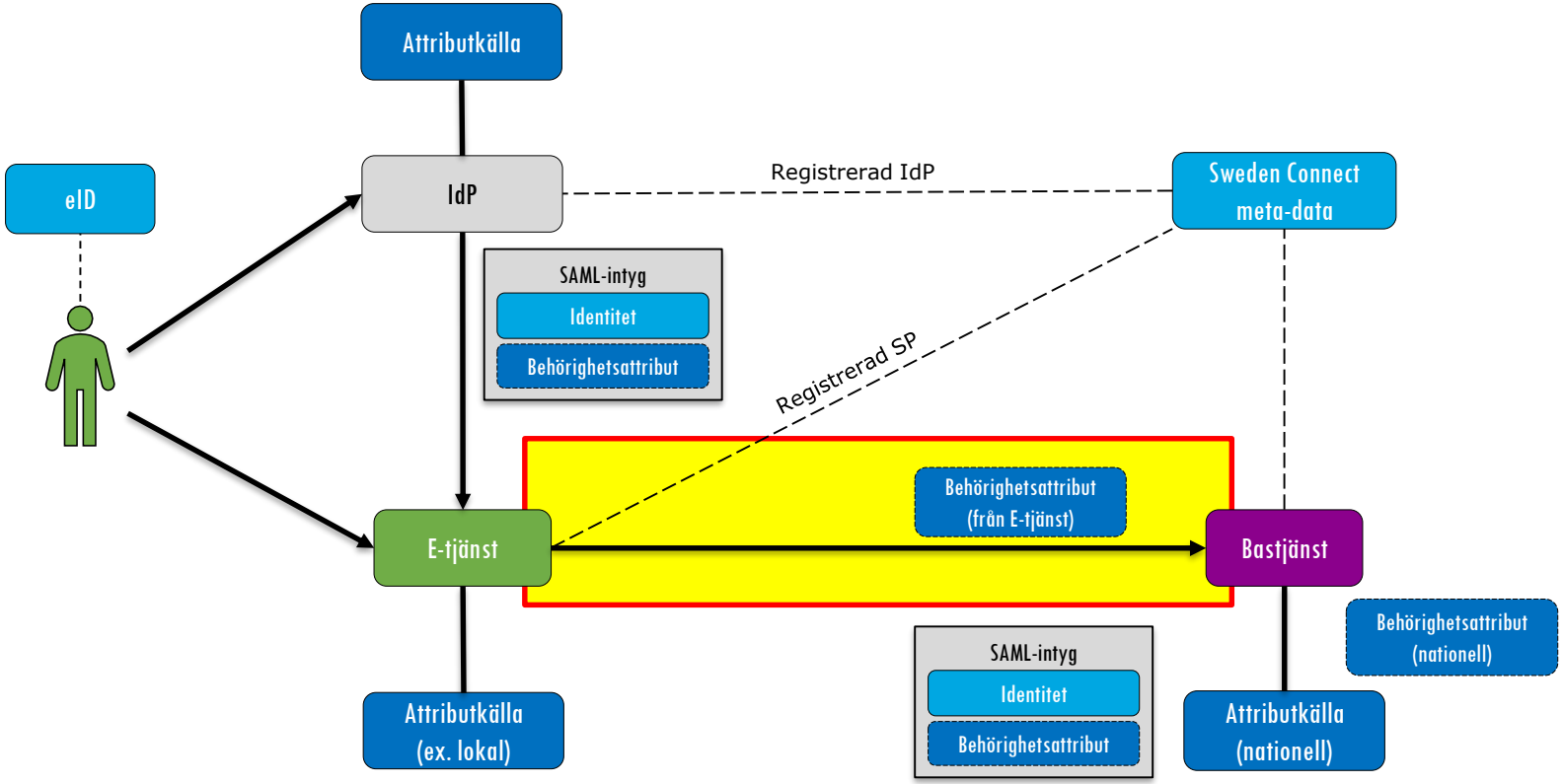
02 - Deployment Profile for the Swedish eID Framework, 6.1 Security Requirements (jan 2020)

The <saml2:Assertion> element issued by the Identity Provider MAY be signed using a <ds:Signature> element within the <saml2:Assertion>.

If a Service Provider requires signed assertions, by assigning the WantAssertionsSigned attribute of its metadata record (see chapter 2.1.2), the Identity Provider MUST sign assertions issued to this Service Provider (as well as the response message as stated above).

Överföring behörighetsstyrande attribut

Vad berörs?


Attributkälla
eID
IdP
Registrerad IdP
Sweden Connect meta-data
SAML-intyg
Identitet
Behörighetsattribut
Registrerad SP
Behörighetsattribut (från E-tjänst)
E-tjänst
Bastjänst
Behörighetsattribut (nationell)
SAML-intyg
Identitet
Behörighetsattribut
Attributkälla (ex. lokal)
Attributkälla (nationell)

Finns frågeställningar som behöver besvaras…

- Hur ska överföringen ske?
  - HTTP-header, del av payload/meddelande etc.
- Struktur och format på överföringen?
  - JWT, XML etc.
- Vilka säkerhetsmekanismer behövs?
  - Finns redan krav på ömsesidig autentisering. (mTLS)
  - Behövs fler? checksumma, signatur etc.

Behöver ske i dialog med framförallt systemleverantörer men även övriga intressenter

eHälsomyndigheten

Exempel

- Önskvärt att separera mellan behörighetsinformation och payload/meddelande
- Önskvärt att använda öppna standards

- JWT token (standard, utbyggbar)
- HTTP-header: X-authorization-data

Exempel (forts.)

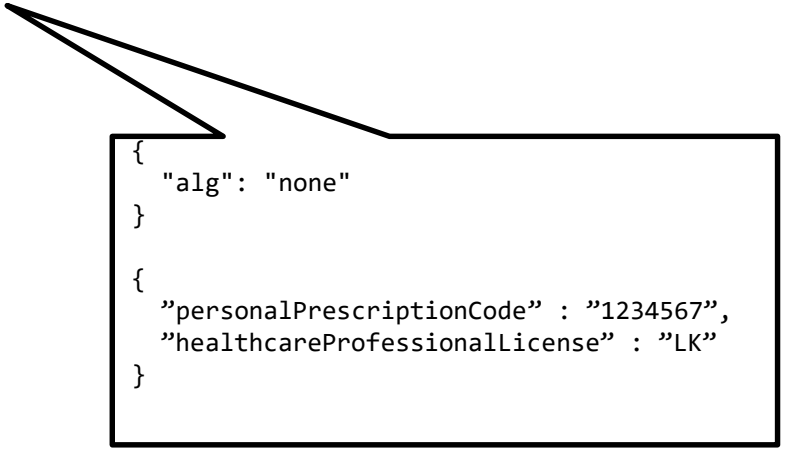
GET / HTTP/1.1

Authorization: Bearer <base 64-encoded: SAML/Oauth2-åtkomst/identitetsintyg>

X-authorization-data: <base 64-encoded: JSON Web Token med attribut>

…

{ ”payload” : ”Hello World!” }



Tack