

Federerad åtkomst

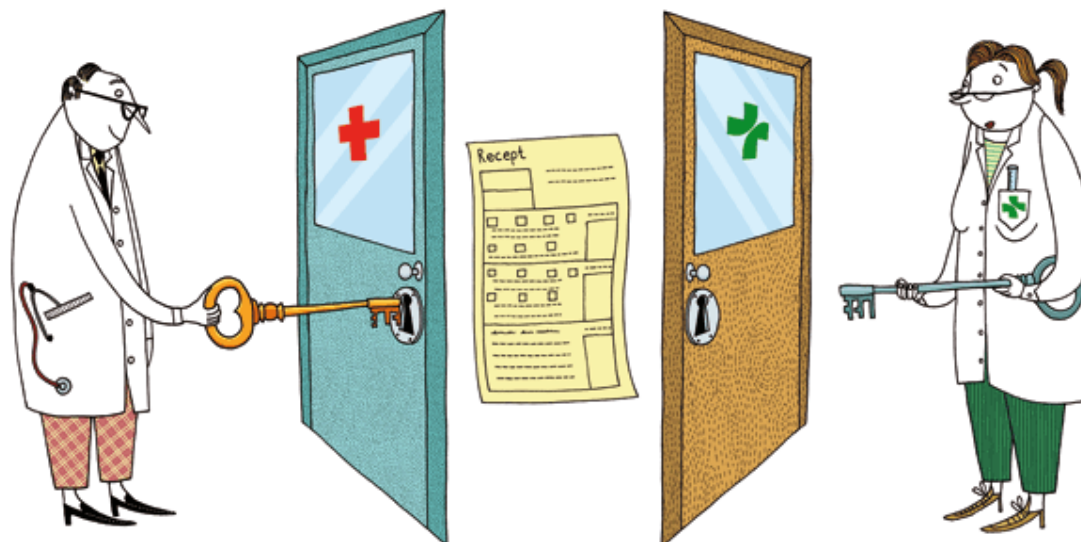
Information om åtkomst till Apotekens Services tjänster inom ramen för en identitetsfederation.

Innehåll

1	Federerad åtkomst till Apotekens Services tjänster	3
1.1	Vad menar Apotekens Service med federation och federerad åtkomst?	3
1.2	Federerad åtkomst med hjälp av SAMLv2.0-baserade intyg	4
	1.2.1 Exempel på aktiviteter och mål	5
1.3	Steg 1 Självdeklarerade egenskaper	6
1.4	Steg 4: Målbild	7
2	Förklaring till SAML och vald intygsmodell	8
2.1	Vad betyder förkortningen SAML	8
2.2	Vilken version av SAML kommer Apotekens Service att stödja?	8
2.3	Intygsmodellens uppbyggnad och funktion	8
2.4	Förklaring till intygsmodellens tre delar	10

1 Federerad åtkomst till Apotekens Services tjänster

Apotekens Service vill kunna erbjuda åtkomst till sina tjänster inom ramen för en identitetsfederering. Detta kommer att möjliggöras bl a genom införandet av en intygsmodell baserad på standarden SAML v2.0.



1.1 Vad menar Apotekens Service med federation och federerad åtkomst?

En federation är en sammanslutning av flera självständiga parter, t ex organisationer där alla deltagande parter gått med på att ingå i ett gemensamt regelverk.

Med federerad åtkomst till Apotekens Service tjänster avses en identitetsfederering där medlemmar har inbördes förtroende för varandras autentiserings- och auktorisationsrutiner.

Förtroendet skapas genom införandet av enhetliga och gemensamma regler baserade på standardmässiga säkerhetsnivåer för identitetsadministration, autentisering, auktorisation och tjänsteleverans.

Exempel: Det är Federationen som definierar kriterierna för t ex stark autentisering och Apotekens Service, i egenskap av tjänsteleverantör, godkänner vilka former av autentisering som är godtagbara för åtkomst till våra tjänster.

Fördelen med en identitetsfederering är bl a att den erbjuder möjligheter att minimera den administrativa kontohanteringen för alla inblandade parter.

För den enskilde användaren innebär det att han/hon autentiseras som vanligt, med lämplig metod för stark autentisering, av sin lokala organisation och ges därefter åtkomst till federationens gemensamma tjänster, t ex till Apotekens Service tjänster.

1.2 Federerad åtkomst med hjälp av SAMLv2.0-baserade intyg

Apotekens Service mål är att kunna erbjuda ett gränssnitt till sina tjänster som möjliggör federerad åtkomst (identitetsfederation) med hjälp av SAMLv2.0 -baserade intyg.

Vägen dit löper över flera år och måste tas i flera steg.

Följande är en vision och angivna datum är endast en uppskattning och inget som är fastställt av Apotekens Service.

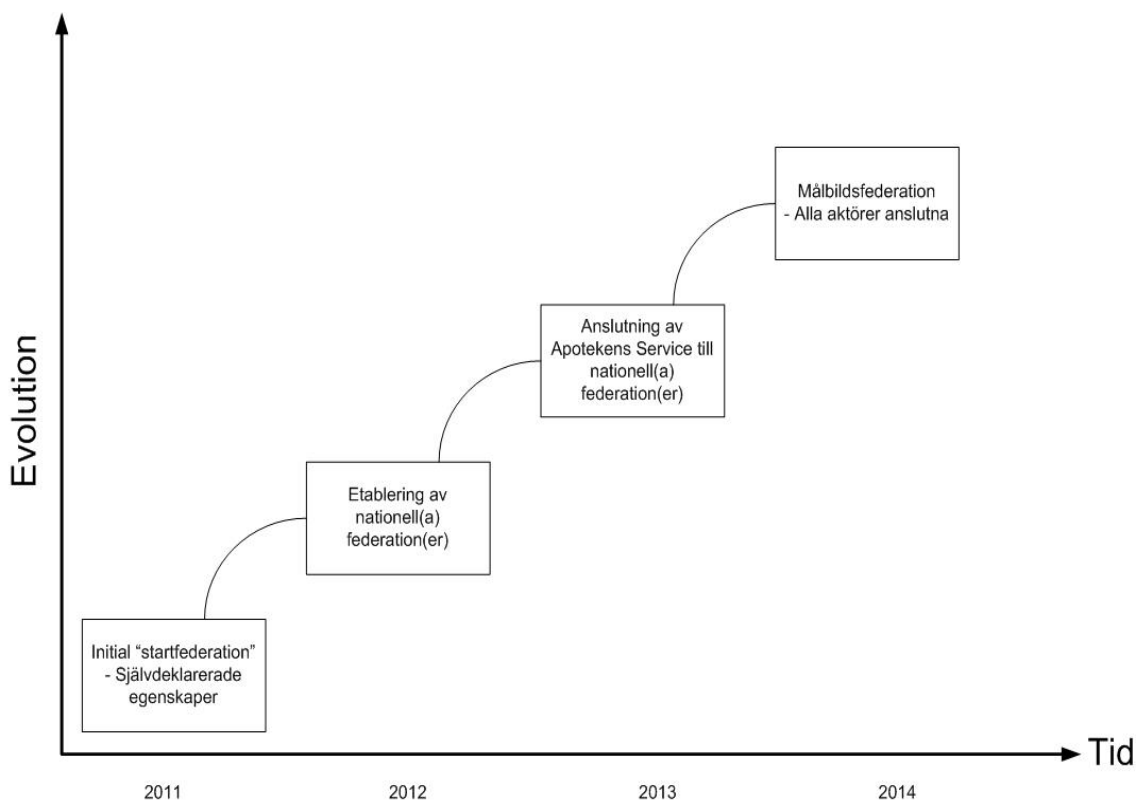


Bild 1: Federationsvision

1.2.1 Exempel på aktiviteter och mål

Steg 1 – 2011

För aktörer:

- Modifiera anropande system för att stödja web service (WS)-anrop
- Utfärda intyg enligt Apotekens Service specifikation
- Kvalitetssäkra intygskällor
- Självdeklaration (egenskaper och tillitsnivåer)

För Apotekens Service:

- Ta fram och kommunicera kravspecifikationer och regelverk
t ex vilka tillitsnivåer som krävs inom federationen för åtkomst till olika tjänster

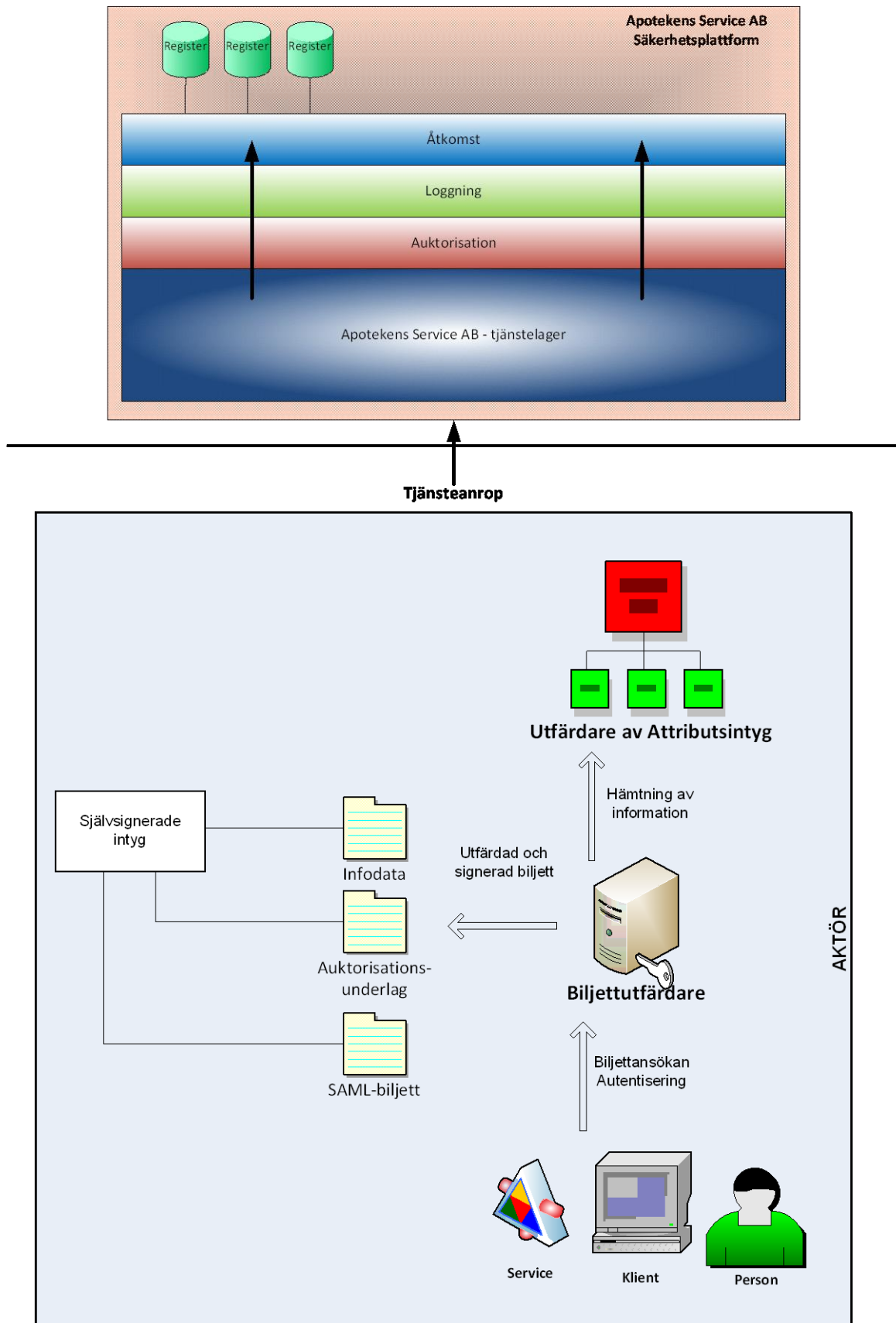
Steg 2 och 3

- Allmänt vedertagna identitetsfederationer etableras, t.ex genom beslut om nationella sådana av E-legitimationsnämnden
- Anpassning av regelverk till fastställda federationspolicys
- Implementering av åtkomst baserat på identifierade tillitsnivåer
- Anslutning av Apotekens Service tjänstegränssnitt mot identitetsfederationer

Steg 4- ca 2014

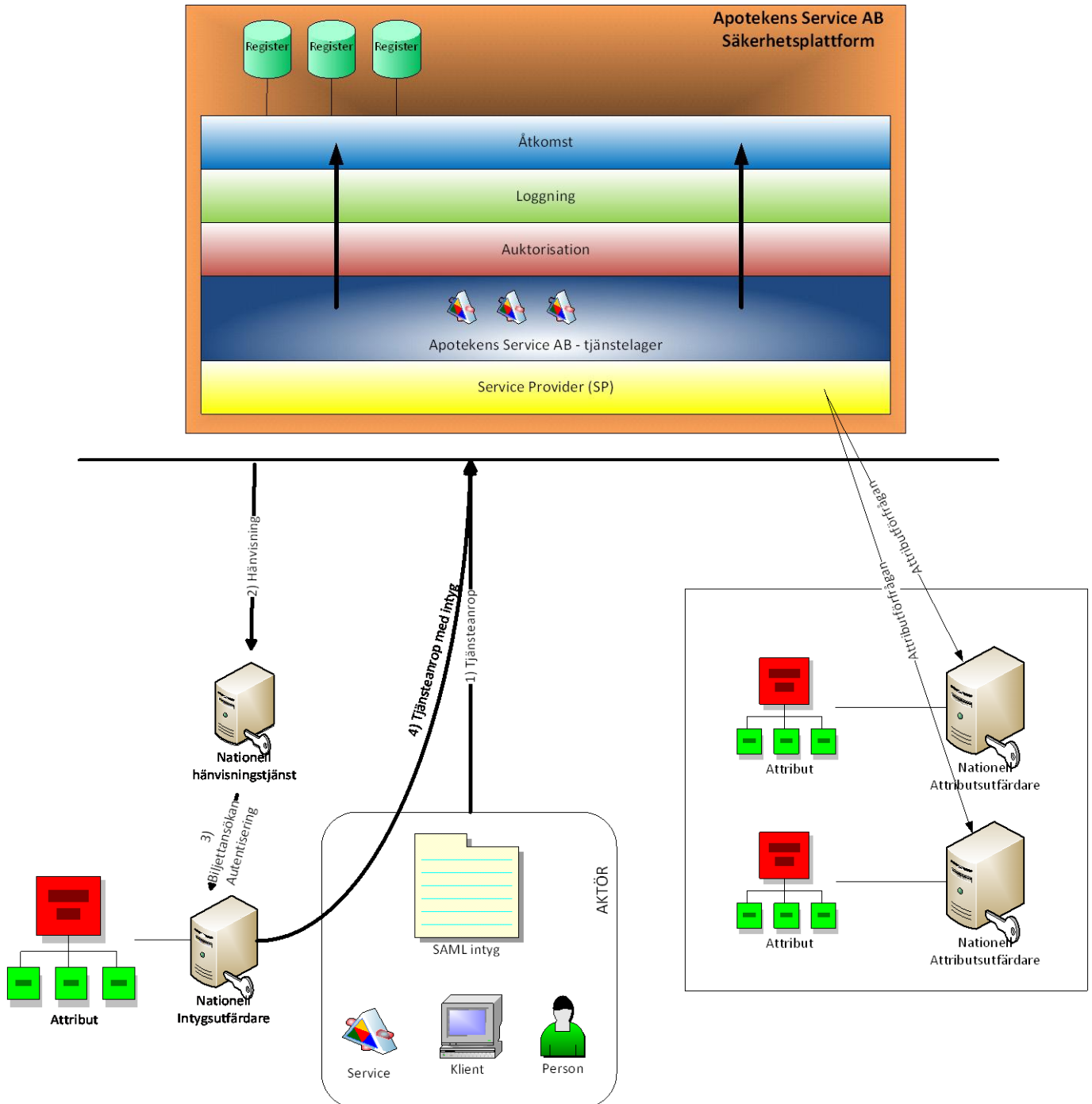
- Aktörer ansluter till identitetsfederationer
- Sann identitetsfederation med dess fördelar

1.3 Steg 1 Självdeklarerade egenskaper



1.4 Steg 4: Målbild

Identitiesfederation med alla aktörer anslutna



2 Förklaring till SAML och vald intygsmodell

2.1 Vad betyder förkortningen SAML

Förkortningen SAML står för Security Assertion Markup Language. Det är en standard som definierats av Organization for the Advancement of Structured Information Standards (OASIS).

SAML är ett standardiserat sätt att definiera och utbyta autentiserings-, attribut- och åtkomstkontrollsinformation i ett format som kallas eXtensible Markup Language (XML).

SAML-standarden är allmänt accepterad och implementerad av leverantörer av webbaserade autentiserings- och åtkomstkontrolltjänster vilket möjliggör bra interoperabilitet.

2.2 Vilken version av SAML kommer Apotekens Service att stödja?

SAML finns i flera versioner. Apotekens Service kommer på sikt endast att stödja SAML v2.0.

2.3 Intygsmodellens uppbyggnad och funktion

Apotekens Service har valt en intygsmodell bestående av tre delar:

1. Autentiseringsunderlag (SAML Assertion).
2. Auktorisationsunderlag (en eller flera underställda SAML-biljetter).
3. Övrig infodata (en eller flera underställda SAML-biljetter. Information som är specifik för respektive tjänst eller som krävs för loggning).

Till autentiseringsunderlaget (SAML-Assertion) knyts ett eller flera intyg för auktorisationsdata och tjänstespecifik infodata. Detta sammantaget ger ett komplett underlag för att säkerställa behörig åtkomst till Apotekens Services tjänster.

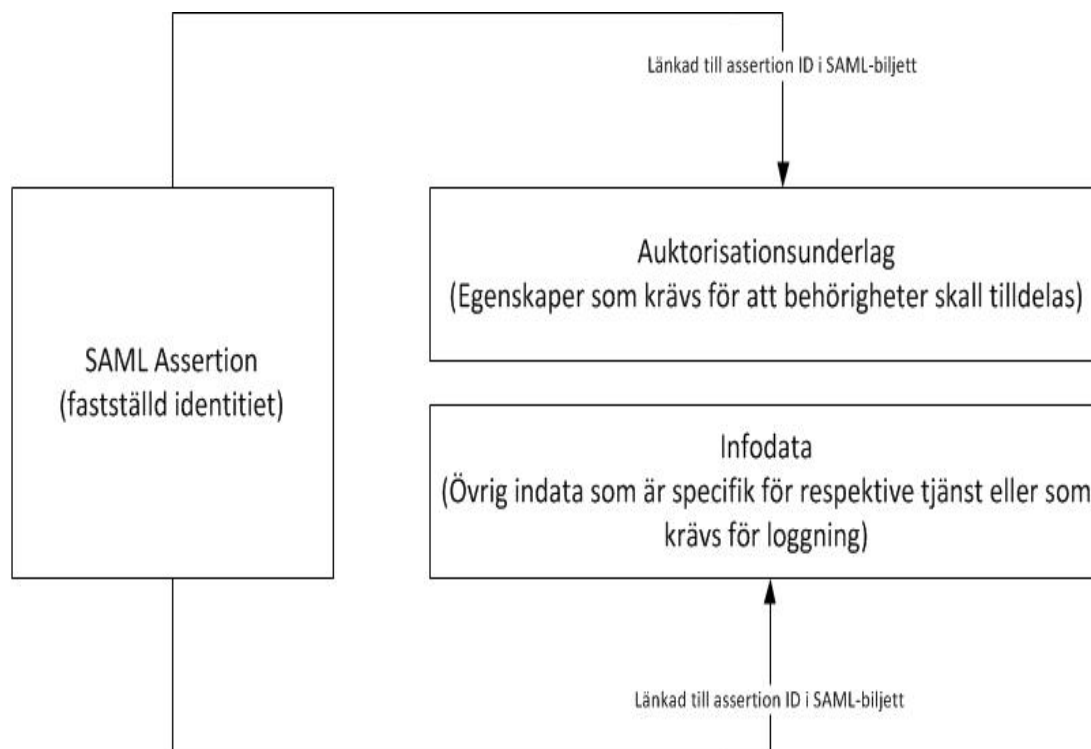


Bild 2: Apotekens Service intygmodell.
Visar relationen mellan autentiserings- auktorisations- och infodata.

2.4 Förklaring till intygsmodellens tre delar

Del 1: SAML Assertion

(fastställd identitet)

Påvisar endast fastställd identitet, dvs autentisering.
(Assertion betyder "påstående" men kan jämföras med en identitetshandling, t ex ett körkort).

Del 2: Auktorisationsunderlag

(egenskaper som krävs för att behörigheter ska tilldelas)

Auktorisationsunderlaget inhämtas, i form av ett eller flera intyg, av en åtkomstkontrolltjänst eller begäras in från brukaren tillsammans med en digital signatur som är godkänd av Apotekens Service.

Samtliga auktorisationsunderlag skall innehålla följande information:

- **Connected Assertion ID:**
information om vilket assertion ID (Identitetshandlingens unika ID) som auktorisationsdata knyts till. Assertion ID kan liknas vid körkortsnumret.
- **Issuer:**
Information om den som utfärdat auktorisationsdata. URL identifierar utfärdarens domän.

Utöver dessa krävda egenskaper kan auktorisationsunderlaget fyllas på efter behov för respektive tjänst.

Exempel på auktorisationsunderlag är, egenskaper såsom:

- Förskrivarkod
- ApoteksID

Del 3. Infodata

(övriga data som är specifik för respektive tjänst eller som krävs för loggning)

För att kunna tillhandahålla information som *inte* har med autentisering eller auktorisation att göra skall ett separat dataobjekt, infodata, användas.

Denna information kan hämtas, i form av ett eller flera intyg, av en åtkomstkontrolltjänst eller begäras in från brukaren tillsammans med en digital signatur som är godkänd av Apotekens Service.

Infodata är ett separat och signerat dataobjekt vilket medger större flexibilitet genom att aktörer kan skilja på identitetsleverantör och infodataleverantör. Respektive tjänst kan begära in olika former av underlag beroende på kraven för respektive tjänst.

Samtliga infodataunderlag skall innehålla följande information:

- **Connected Assertion ID:**
information om vilket assertion ID (Identitetshandlingens unika ID) som auktorisationsdata knyts till. Assertion ID kan liknas vid körkortsnumret.
- **Issuer:**
Information om den som utfärdat infodatat. URL identifierar utfärdarens domän.

Utöver dessa krävda egenskaper kan infodata fyllas på efter behov för respektive tjänst.

Exempel på infodata är egenskaper såsom:

- Aktiva val (t.ex. om brukaren har flera roller).
- Systeminformation (t.ex. IP-adress).