

Apotekens Service Federationsmodell

*Detta dokument beskriver hur Apotekens Service samverkar inom
identitetsfederationer*

Innehåll

1	Syfte med detta dokument	3
2	Definitioner	3
3	Apotekens Service principer för att samverka i identitetsfederationer	4
3.1	Åtkomst till tjänster kräver anslutning till identitetsfederation	4
3.2	Två scenarier för åtkomst till Apotekens Service tjänster	4
3.2.1	Åtkomst via web service - scenario 1	4
3.2.2	Åtkomst webbapplikationer - scenario 2	6
4	Attribut och applicering av behörigheter	7
5	SAML	10
5.1	Signering av intyg	11
5.2	Kryptering av intyg	11
5.3	Intygens giltighetstid	11
6	Intygstransport mot Apotekens Service	13
6.1	Web Service scenariot	13
6.2	Webbapplikationsscenariot	14
7	Tillitsnivåer uttryckt i ett SAML-intyg	15
	Revisionshistorik	15
	Bilaga 1 – Integration mot Vårdens Nationell Tjänsteplattform	16

1 Syfte med detta dokument

Alla former av åtkomst till Apotekens Service tjänster skall autentiseras i enlighet med de lagar och förordningar som Apotekens Service är skyldiga att upprätthålla. Autentisering skall ske i enlighet med den tillitsnivå som Apotekens Service kopplat till olika former av åtkomst. Tillitsnivåer används för att beskriva den grad av tillit (övertygelse) som en tjänsteleverantör, t ex Apotekens Service, kan sätta till att en tjänstenyttjare faktiskt är den som den utger sig för att vara.

Apotekens Service modell för tillitsnivåer är baserad på Kantara Identity Assurance Framework samt kommande ISO standard ISO/IEC CD 29115.

För information om Kantara Identity Assurance Framework, se följande länk:

<http://kantarainitiative.org/>

För åtkomst till information som av Apotekens Service klassificeras som konfidentiell, t ex känsliga personuppgifter, krävs att tillitsnivå tre, dvs. hög grad av tillit till identiteten, uppnås.

2 Definitioner

Autentisering – Verifiering av uppgiven identitet

Autentiseringsmetod – Metod för att verifiera uppgiven identitet

Auktorisation – Fastställande av åtkomsträttigheter för en användare till olika systemresurser

Kryptering – Metod för att skydda information med hjälp av en nyckel och en algoritm

Tillförlitlighet – Mått på i vilken grad någon levererar information av den kvalitet den säger sig leverera

IDP – Identity Provider (identitetsintygutfärdare), den kombinationer av hård- och mjukvara som utfärdar identitets- och attributintyg.

SP – Service Provider (tjänsteleverantör), den kombination av hård- och mjukvara som agerar federationsgränssnitt för en viss tjänst.

SAML Assertion – Se SAML-intyg

SAML-Intyg – Identitets- eller attributintyg som följer SAML-standard och som påvisar identitet och/eller egenskaper för ett namngivet subjekt

SAML-Biljett – Se SAML-intyg

3 Apotekens Service principer för att samverka i identitetsfederationer

3.1 Åtkomst till tjänster kräver anslutning till identitetsfederation

Apotekens Service har inte för avsikt att etablera någon egen separat identitetsfederation utan kommer att ansluta sina tjänster till ett antal identitetsfederationer som etableras på nationell eller internationell basis. För att få åtkomst till Apotekens Service tjänster måste nyttjaren av tjänsterna vara ansluten till någon av dessa identitetsfederationer.

Gemensamt för samtliga federationer som Apotekens Service avser att ansluta till är att dessa applicerar ett adekvat tillitsramverk.

Endast intyg som är utfärdade av intygsutfärdare som är certifierade för minst tillitsnivå tre accepteras av Apotekens Service.

Apotekens Service kommer inte att certifiera identitetsutfärdare som används inom ramarna för olika identitetsfederationer.

3.2 Två scenarier för åtkomst till Apotekens Service tjänster

Scenario 1: Web services

Apotekens Service tillhandahåller de flesta tjänsterna i web service format för anslutna aktörer, vilka tecknat tjänsteavtal. I dessa fall ligger slutanvändarinteraktionen i system utanför Apotekens Service ansvarsområde och kontroll.

Scenario 2: Webbläsare

I undantagsfall erbjuder Apotekens Service åtkomst till applikationer genom vilka en slutanvändare interagerar direkt gentemot via en webbläsare. Dessa webbapplikationer har ett annorlunda federationsscenario. Skillnaden mellan dessa scenarion beskrivs nedan.

3.2.1 Åtkomst via web service - scenario 1

För att en aktör skall kunna genomföra ett lyckat tjänsteanrop mot Apotekens Service tjänster skall identiteten på slutanvändaren uppvisas tillsammans med de egenskaper som krävs för aktuellt åtkomstförsök. Respektive tjänst kan ha olika behov av egenskaper, något aktörer skall beakta vid anslutning till Apotekens Service tjänster.

Det intygsformat som används är Security Assertion Markup Language (SAML), vilket definierats som standard av Organization for the Advancement of Structured Information Standards (OASIS). Apotekens Service AB stödjer endast SAML v2.0. Apotekens Service stödjer endast intyg som ställs ut som persistent.

Vidare kommer Apotekens Service endast att agera inom federationer som publicerar och hanterar SAML Metadata på ett sätt som ligger i linje med Apotekens Service tolkning av tillitsnivå tre (eller nivå fyra).

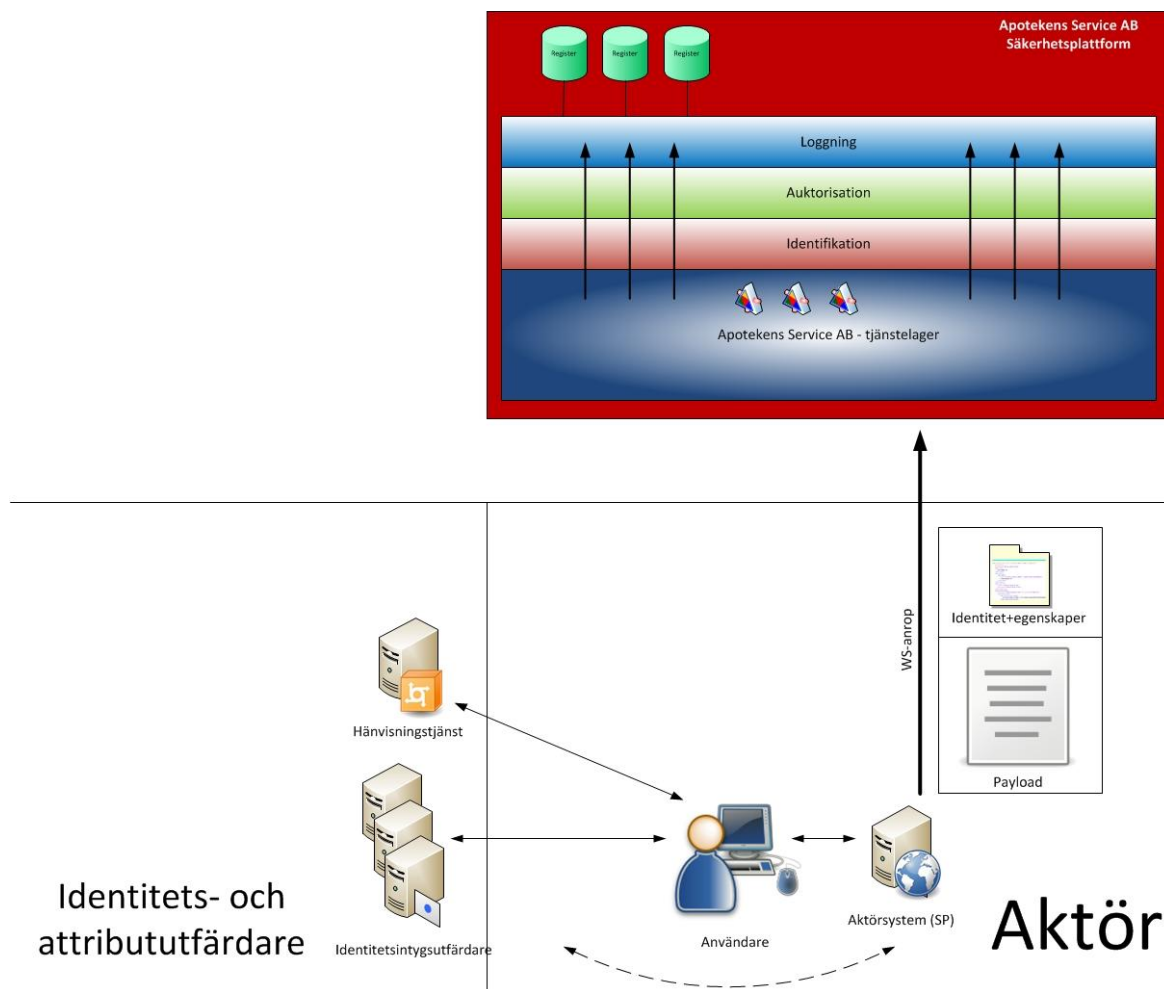
Apotekens Service AB kommer inte att nyttja SAML för att hantera data som är knuten till själva tjänsterna utan endast använda dessa för identifikation, auktorisation samt i loggsyfte. Tjänsteknuten information hanteras som en del av tjänsternas meddelande-”payload”.

I tjänster som tillhandahålls via web services finns ingen aktiv SAML-profil mellan aktörssystemet och Apotekens Service tjänstegränssnitt. Istället implementeras SAML-profiler hos aktören i form av en eller flera SAML SP(s) (Service Provider) samt genom att Apotekens Service tjänstegränssnitt tillämpar relevant federations SAML Metadata.

Aktörssystemet agerar SAML endpoint gentemot berörda federationer via den/de SP(s) som etablerats för att kvittera ut identitetsintyg samt attributintyg.

Apotekens Service tjänstegränssnitt agerar sekundär SP gentemot aktörssystemet, som mottagare och verifieringspart för de intyg som aktören skickar in som en del av ett tjänsteanrop.

Följande bild beskriver övergripande hur Apotekens Service web service tjänster kan nås inom ramarna för federativa förhållanden.



Figur 1 – Åtkomst till web service tjänster

Intyg samlas och paketeras i det meddelandeformat som Apotekens Service använder sig av, detta ansvar ligger på aktörens sida. Observera att det är aktörssystemet som ansvarar för att tillämpa SAML-profil(er) gentemot den/de federationer aktören verkar inom för att kunna kvittera ut identitets- och attributsintyg som används vid anrop mot Apotekens Service tjänster. Aktören är också ansvarig för att intyg innehåller egenskaper som krävs för åtkomst till Apotekens Service tjänster.

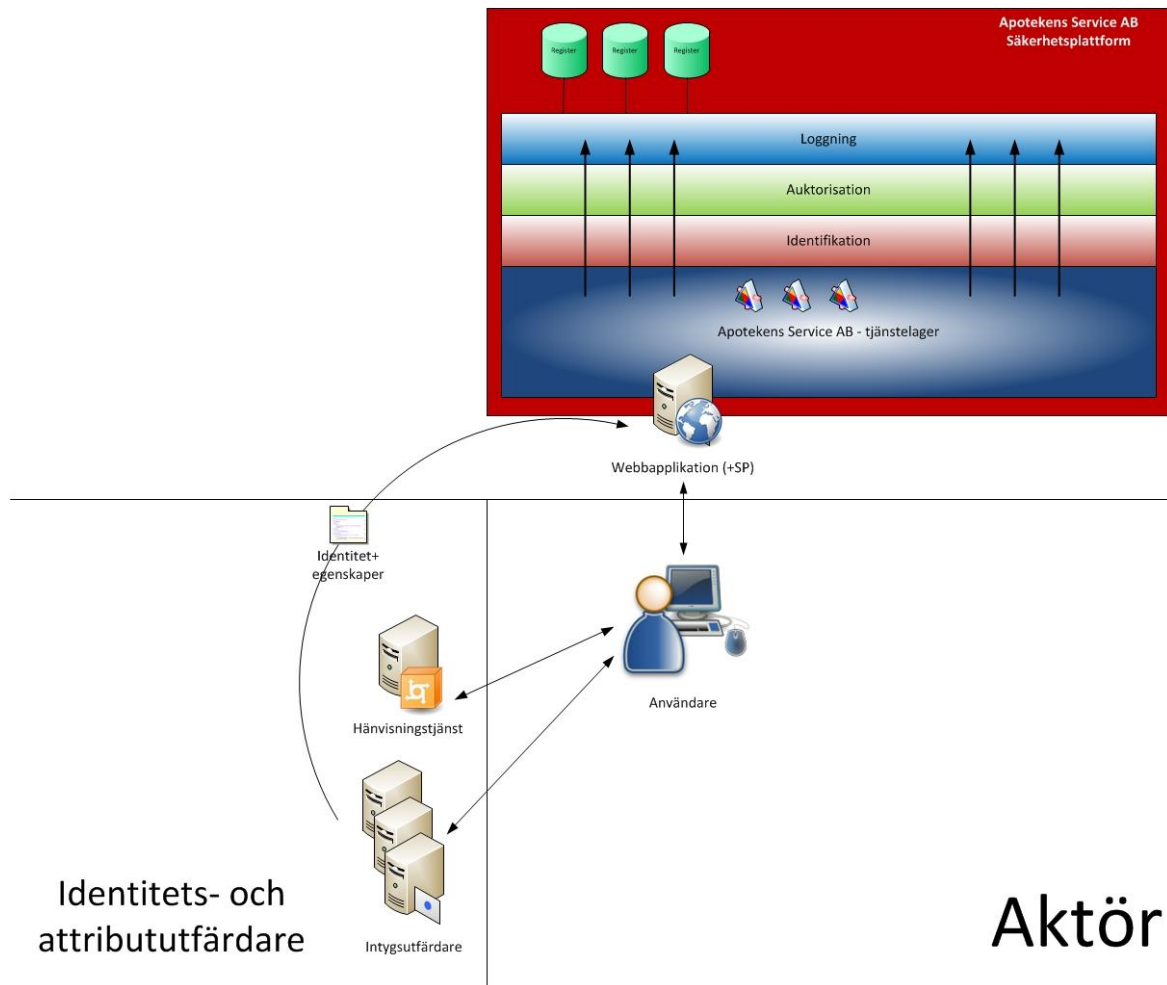
3.2.2 Åtkomst webbapplikationer - scenario 2

I de fall Apotekens Service implementerar sina tjänster som webbapplikationer och kommer i direktkontakt med slutanvändaren finns en aktiv SAML-profil mellan identitetsintygutfärdare och Apotekens Service tjänstegränssnitt. I detta scenario har även Apotekens Service möjlighet att ställa aktiva SAML-attribut frågor för att hämta in attribut enligt behov, då t.ex. identitetsintyg saknar krävda attribut. Det senare är under förutsättning att erforderliga attributfärdare har möjlighet att utfärda attributintyg med de attribut Apotekens Service är intresserade av.

Apotekens Service avser att implementera Kantara eGovernment 2.0 SAML Profile som primär SAML-profil men bevakar eventuella andra SAML-profiler som används inom de federationer Apotekens Service avser att verka inom.

Apotekens Service tjänstegränssnitt agerar SAML endpoint gentemot den/de federationer Apotekens Service verkar inom via den/de SP(s) som etableras för att kvittera ut identitetsintyg samt attributintyg. Apotekens Service tjänstegränssnitt tillämpar även SAML Metadata för de federationer som Apotekens Service verkar inom.

Följande bild beskriver övergripande hur Apotekens Service webbapplikationer kan nå inom ramarna för federativa förhållanden.



Figur 2 – Åtkomst till webbapplikation

4 Attribut och applicering av behörigheter

Apotekens Service applicerar behörigheter till sina tjänster baserat på egenskaper som respektive tjänstenyttjare visar upp före åtkomst. Denna egenskapsbaserade behörighetstilldelning applicerar behörigheter mot att följande uppvisas av tjänstenyttjare:

- En godkänd identitet
- De behörighetsgivande egenskaper som tjänsten i fråga kräver och som är knutna till tjänstenyttjaren i fråga

Samtliga egenskaper som krävs för respektive tjänst redovisas av Apotekens Service i samband med tecknande av tjänsteavtal.

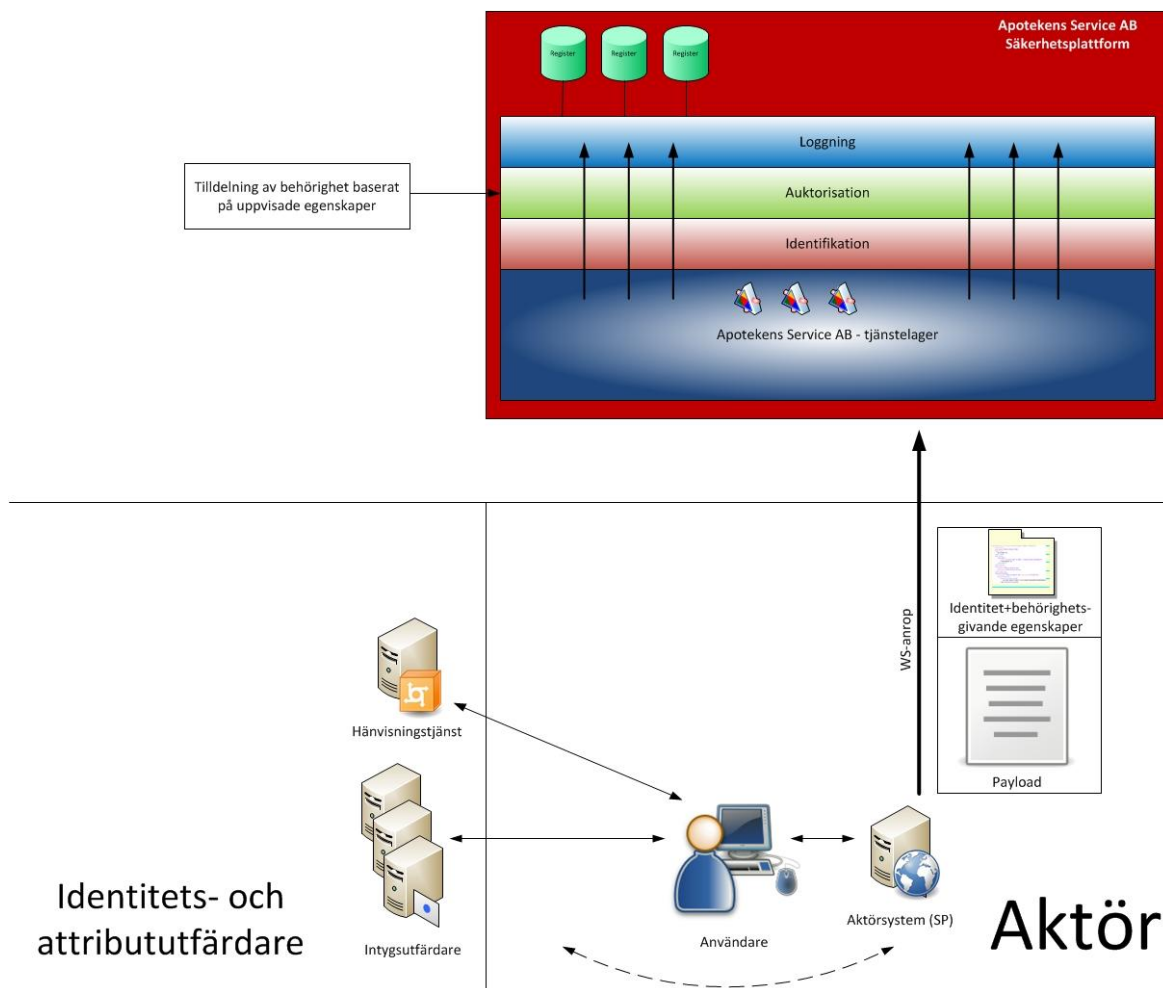
Samtliga behörighetsgivande attribut skall levereras via SAML-intyg som kommer från betrodd intygsutfärdare.

Attribut ska levereras på något av följande sätt:

1. Som SAML attributstatement som en del av utfärdat identitetsintyg på minst tillitsnivå tre
2. Som SAML attributstatement utfärdade inom ramarna av ett eller flera attributsintyg,

För attributsintyg och identitetsintyg gäller att dessa skall vara digitalt signerade av utfärdande IDP samt att de ej får modifieras i något skede efter utfärdande.

Vilka attribut som krävs för åtkomst är beroende på vilken tjänst som anropas. Apotekens Service tilldelar behörigheter i enlighet med respektive tjänsts regler för åtkomst.



Figur 3 – Tilldelning av behörigheter baserat på uppvisade egenskaper

Det attributcentrerade förhållningssättet möjliggör för tjänstenyttjare att använda en elektronisk legitimation som påvisar en unik identitet i enlighet med minst tillitsnivå tre. Behörighetsgivande egenskaper kan därefter tilldelas identiteten av betrodda attributfärdare, med andra ord behöver inte nödvändigtvis legitimationsutfärdaren agera utfärdare av behörighetsgivande attribut.

För aktörer som definierar behörighetsgivande egenskaper i form av roller kan detta översättas till egenskaper då en roll kan formars av en eller flera egenskaper. Apotekens Service definition av en åtkomstgivande roll är en tydligt definierad och sammansatt samling egenskaper som knyts till det tjänstenyttjande subjektet.

Exempel på hur behörigheter kan appliceras mot uppvisade egenskaper:

- Apotekens Service tjänst X kräver att tjänstenyttjaren uppvisar egenskaperna zzz samt yyy inom ramarna för uppvisade SAML-intyg för att tilldelas en viss behörighet. SAML-intygen behöver då uppvisa följande exempelegenskaper för att behörigheter skall tilldelas tjänstenyttjaren:

```
<AttributeStatement>
```

```
<Attribute Name="urn:zzz:names:federation:attributeName:zzz "  
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
```

```
<AttributeValue>VärdeX</AttributeValue>
```

```
</Attribute>
```

```
<Attribute Name="urn:zzz:names:federation:attributeName:yyy"  
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
```

```
<AttributeValue>VärdeY</AttributeValue>
```

```
</Attribute>
```

```
</AttributeStatement>
```

Uppvisade egenskaper (zzz samt yyy i exemplet ovan) tilldelar tjänstenyttjaren behörighet i tjänst X.

5 SAML

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

Den huvudsakliga uppgiften är att tillhandahålla interoperabilitet mot autentiserings- och åtkomstkontrolltjänster.

Huvuddelarna av SAML inkluderar nedanstående:

Assertions: Assertions kan översättas med intyg, försäkran eller påståenden som rör säkerhet. SAML definierar tre typer av intyg, vilka är deklarerationer för en eller flera fakta knutna till ett system eller en person.

- **Autentiseringintyg** (Authentication statement) av vilket följer att systemet eller personen kan styrka sin identitet.
- **Egenskapsintyg** (Attribute statement) innehåller specifika egenskaper knutna till systemet eller personen, t.ex. organisationstillhörighet.
- **Rättighetsbeslutsintyg** (Authorization decision statement) förmedlar vad systemet eller personen får lov att göra (t.ex. tillåtelse att läsa ett visst register). Apotekens Service tillämpar ej denna typ av intyg eftersom behörigheter tillämpas på uppvisade attribut.

Request/response protocol: Dessa protokoll definierar hur SAML frågar efter och får svar på de intyg som är knutna till systemet eller personen.

Bindings: Denna del av SAML definierar exakt hur request- och responsprotokollet och intygen mappar in i olika transportprotokoll (t.ex. SOAP).

Profiles: Profiler anger på vilket sätt SAML assertions med hjälp av transportprotokollen kan utbytas mellan de kommunicerande parterna.

5.1 Signering av intyg

För att intyg skall vara giltiga måste de signeras av aktuell IDP. Genom signeringen säkerställs att intyget inte har manipulerats sedan det utfärdats.

Andra IT-tjänster kan därefter lita på innehållet i intyget om dessa IT-tjänster har ett trustförhållande till utfärdande IDP.

Detta sker genom en teknisk trust till det SAML Metadata för den federation som IDPn verkar inom.

5.2 Kryptering av intyg

Intyg skall krypteras i samtliga transportskeenden gentemot Apotekens Service .

Åtkomst via web service - scenario 1

Kryptering skall alltid ske på transportnivå och föregås av autentisering av mottagaren via TLS-protokollet (i form av Mutual TLS). Det får inte skickas några intyg som är krypterade på intygsnivå till Apotekens Service.

Åtkomst webbapplikationer - scenario 2

I webbapplikationsscenario 2 stödjer Apotekens Service följande krypteringsförhållanden:

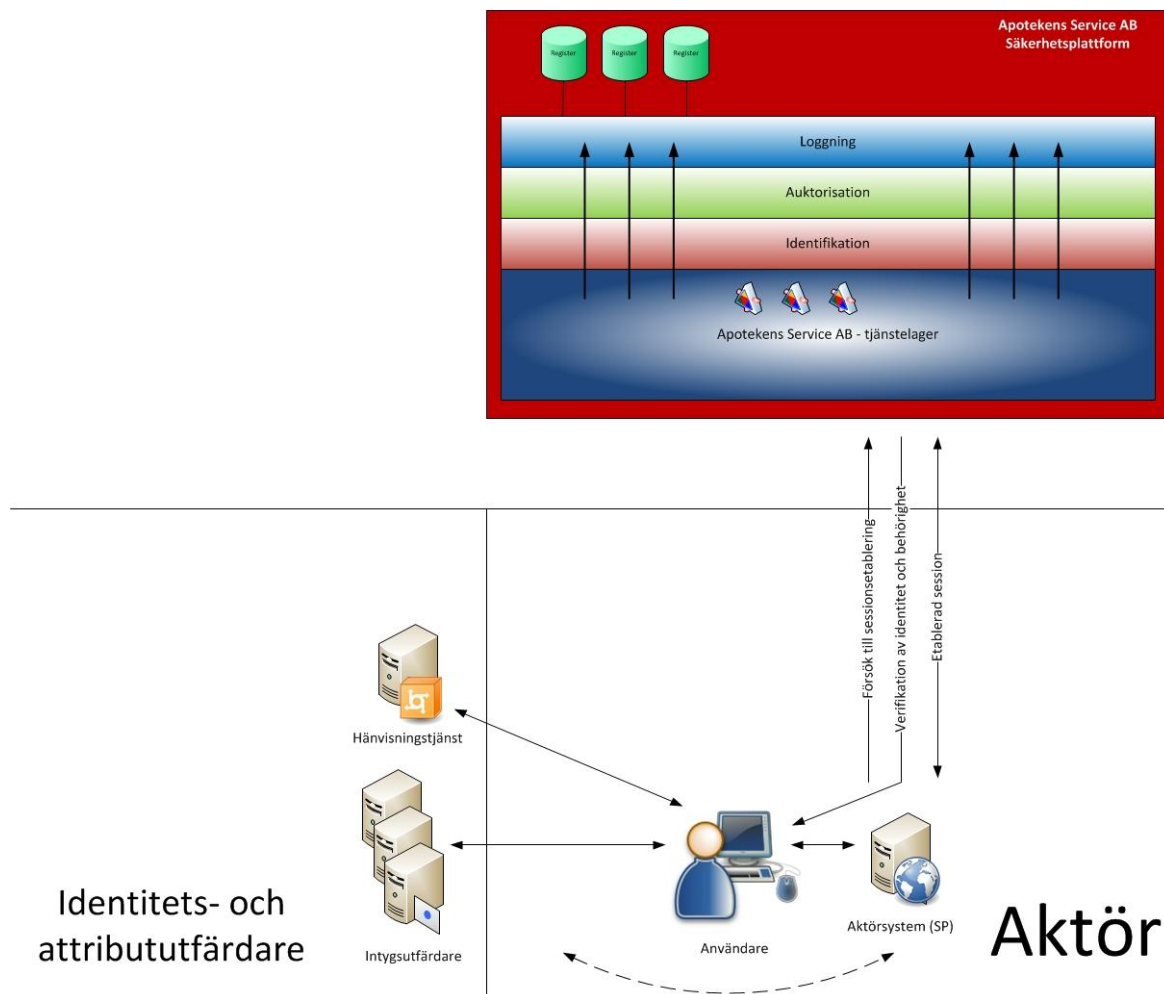
- Kryptering på intygsnivå under förutsättning att intyget är krypterat med Apotekens Service publika nyckel.
- Kryptering av intyg på transportprotokollsnivå (TLS).

5.3 Intygens giltighetstid

När ett intyg skapas, sätts en giltighetstid av aktuell IDP. Denna giltighetstid verifieras av Apotekens Service vid etablering av tjänstesession, intyg vars giltighetstid har passerat accepteras ej. Vid tjänsteanrop inom ramarna för befintlig tjänstesession kontrolleras inte intygens giltighetstid.

Då en tjänstesession etablerats kommer inga kontroller av intygens giltighetstid att utföras förrän sessionen avslutas och en ny session etableras. En session etableras för en kombination av aktörssystem och användare (eller system i det fall det är ett tjänsteanrop som görs för ett systems räkning) vilket gör att varje unik användare/system får en separat tjänstesession gentemot Apotekens Service tjänster.

En session löper över en given tid som dikteras av Apotekens Service för respektive tjänst. Då en session löper ut och nya tjänsteanrop behöver göras skall en ny session etableras och nya kontroller på intygens innehåll och giltighet utförs.



För integration mot vårdens Nationella Tjänsteplattform, se bilaga 1 för information om speciellt undantag.

6 Intygstransport mot Apotekens Service

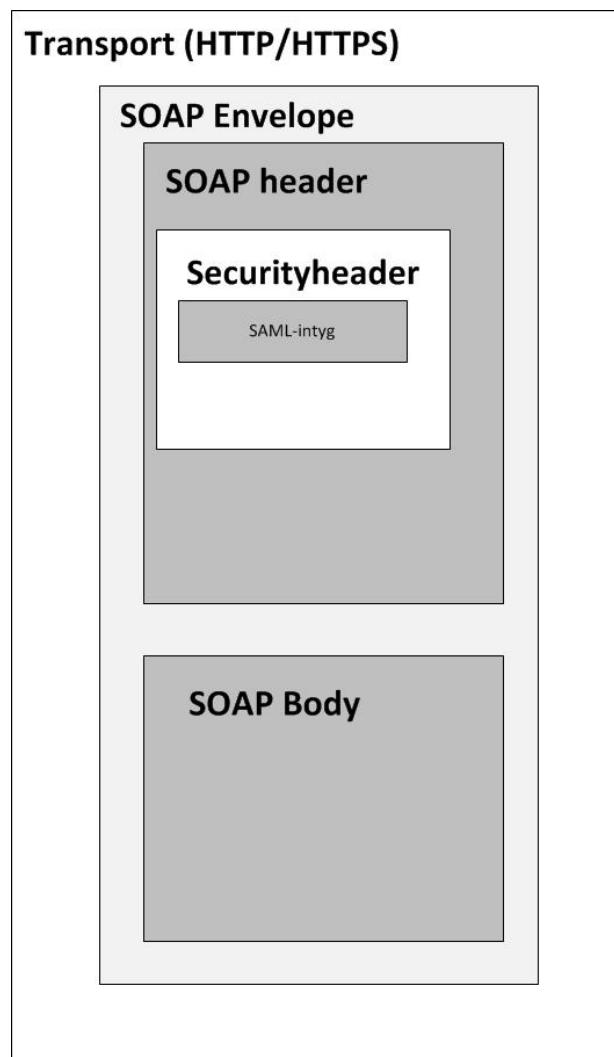
6.1 Web Service scenariot

Aktörer förväntas knyta SAML-intyg till de tjänstemeddelanden som används mot Apotekens Service tjänster.

Här beskrivs hur ett utfärdat intyg knyts till ett SOAP-meddelande.

SAML-intyg skall alltid skickas i oförändrad form. Detta skall ske i ett SOAP-meddelande i ett SOAP-meddelandes header. Närmare preciserat i headerns security-sektion. Se bild nedan.

I SOAP-headern kan även annan information ligga och meddelandet störs inte av detta, utan intyg samverkar ofta med den andra informationen. Exempel på detta är XML-signaturer och XML-kryptering som också kan ligga inom SOAP-headersektionens <Security>-taggar.



Figur 4 – SAML-transport mot Apotekens Service web service tjänster

6.2 Webbapplikationsscenariot

Eftersom Apotekens Service i detta scenario direkt interagerar med slutanvändaren och intygsutställare (IDP) knyts aktiva SAML-profiler direkt mot Apotekens Service tjänstegränssnitt (SP). Apotekens Service agerar i detta läge som en aktiv SP. En aktiv SAML-profil innebär i detta sammanhanget att tjänstegränssnittet aktivt interagerar med både slutanvändaren och intygsutfärdare samt tillämpar autentiseringsföraranden gentemot den/de IDP(er) som utfärdar identitets- och attributintyg för slutanvändaren. Även själva intygstransporten dikteras av den SAML-profil som etableras av SP och IDP i detta fall.

Intygstransporten skall ske i linje med den SAML-profil¹ som Apotekens Service tillämpar i sin SP gentemot de federationer man verkar inom.

¹primärt Kantara e-Government SAML Profile 2.0

7 Tillitsnivåer uttryckt i ett SAML-intyg

På intygsnivå kan en tillitsnivå² kopplas till ett intyg på samma sätt som exempelvis en autentiseringsmetod, genom nyttjandet av AuthnContextClassRef-elementet i intyget. Själva namespace för ett level of assurance framework är dock specifikt för respektive framework och inte en del av SAML 2.0-schemat. Ett exempel på hur en tillitsnivå kan implementeras inom ramarna för AuthnContextClassRef-elementet:

```
urn:oasis:names:tc:SAML:2.0:post:ac:classes:zzz-ramverk:v1-0-2:level3
```

Ovanstående exempel visar hur det går att beskriva att intyget är utfärdat på nivå 3 i enlighet med zzz-ramverk version 1-0-2.

Revisionshistorik

Utgåva	Datum	Kommentar
1.0	2011-12-12	

² Apotekens Service modell för tillitsnivåer är baserad på Kantara Identity Assurance Framework samt kommande ISO standard ISO/IEC CD 29115 (ref.xx).

Bilaga 1 – Integration mot Vårdens Nationell Tjänsteplattform

Följande speciella undantag gäller enligt överenskommelse med Cehis:

- Eftersom vården i dagsläget ej förnyar utfärdade SAML-intyg då dess giltighetstid har passerat accepterar Apotekens Service intyg från vården som passerat sin giltighetstid vid etablering av tjänstesessioner från vården, dock som längst 8 timmar efter att intygens giltighetstid startar.