

Krav på identifiering för åtkomst till konfidentiell information

Apotekens Service tillämpning av tillitsnivå tre, baserat på Kantara Identity Assurance Framework, för åtkomst till känsliga personuppgifter.

Innehåll

1	Inledning	3
2	Definitioner	3
3	Apotekens Service tillitsnivåer	4
4	Accepterade certifieringsinstanser	4
5	Kriterier som utvärderas för tillitsnivå tre	5
5.1	Attributsutfärdare	6
6	Exempel på relationen mellan olika utvärderingskriterier	6
7	Sammanfattning av tillitsnivåer och exempel på användningsområden	8
8	Bilaga 1 – Exempel på utvärderingskriterier för tillitsnivå tre	9
8.1	Administrativa krav	9
8.2	Krav på handhavande (Operationella krav)	11
8.3	Tekniska krav	11
9	Bilaga 2 – Exempel på olika former av autentiseringsmetoder i olika tillitsnivåer	13
10	Revisionshistorik	15

1 Inledning

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.

Detta dokument beskriver Apotekens Service tillämpning av tillitsnivå tre.

2 Definitioner

Definitioner av begrepp som används inom ramarna för detta dokument:

Dessa begrepp är definierade i enlighet med SOU 2010-104 samt översättning av OASIS SAML-specifikationer: <http://www.oasis-open.org/>

Begrepp	Betydelse
Identitetsutfärdare	Den som utfärdar identitetsintyg inom infrastrukturen för identifiering.
Attributsutfärdare	Attributsutfärdare; den som utfärdar attributsintyg inom infrastrukturen för identifiering eller en annan anknytande infrastruktur.
E-tjänsteleverantör	Den part som tillhandahåller en e-tjänst som använder identitets- och attributintyg.
Identitetsintyg	Identitetsintyg; ett av en identitetsutfärdare utställt intyg i elektronisk form med uppgifter om en användares identitet och attribut.
Attributsintyg	Attributsintyg; ett av en attributsutfärdare utställt intyg i elektronisk form med uppgifter om användares juridiska behörighet, organisatoriska roll eller andra egenskaper.
Tillitsnivå	Tillitsnivå; den skyddsklass till vilken en elektronisk legitimation hänförs.
Identitetsintygsutfärdare	Den kombination av hård- och mjukvara som behövs för att ställa ut identitetsintyg för en identitetsutfärdares räkning.
IDP	Identity Provider, se identitetsintygsutfärdare.

Begrepp	Betydelse
SP	Service Provider, den kombination av hård- och mjukvara som tjänsteleverantörer tillämpar aktiva SAML-profiler mot den/de federationer inom vilken/vilka man verkar.
SAML	Security Assertion Markup Language, ett tekniskt standardprotokoll för identitets- och attributsintyg.
CA	Certificate Authority, utfärdare av digitala certifikat som påvisar en specifik identitet (en person, en tjänst, en organisation etc.).
Identitetsfederation	En konvergens av regler och infrastruktur för att möjliggöra identifikation av personer, tjänster och organisationer mellan olika parter som litar på varandra samt federationens ägare.

3 Apotekens Service tillitsnivåer

Apotekens Service tillämpar tre tillitsnivåer, enligt nedanstående.

Tillitsnivå fyra används inte i dagsläget eftersom den inte kan appliceras på några publika och befintliga identitetsutfärdare i Sverige.

Detta dokument beskriver endast tillitsnivå tre som är relevant för åtkomst till konfidentiell information, t ex receptuppgifter.

Tillitsnivå	Beskrivning
1	Minimal eller obefintlig tillit till identitetens äkthet
2	Viss tillit till identitetens äkthet
3	Hög tillit till identitetens äkthet

Se bilaga 1 för exempel på utvärderingskriterier för tillitsnivå tre.

4 Accepterade certifieringsinstanser

Apotekens Service utför inte certifiering av identitetsutfärdare med tillhörande identitetsintygsutfärdare.

Identitetsutfärdare förväntas bli certifierade och granskade av en tredje part med ackreditering för tillitsnivå tre, dvs med erforderlig erfarenhet och kunskap om

- Kantara Identity Assurance Framework,

- ISO standard ISO/IEC CD 29115 (kommande)
- certifiering

Följande certifieringsinstanser accepteras av Apotekens Service:

- XXXX¹
- YYYY

5 Kriterier som utvärderas för tillitsnivå tre

Tillitsnivåer för identitetsintyg baseras på identitetsutfärdarens:

- Teknik, dvs teknisk implementation, såsom bärare av identiteter eller identitetsintygsutfärdarens kryptografiska nyckelhantering.
- Administration, dvs administrativa regler och rutiner som används för livscykelhanteringen av identiteter
- Handhavande, dvs operationella rutiner som tillämpas

Tillitsnivåerna formas genom kombinationen av dess tre delar. Dessa aspekter utvärderas som helhet och bildar tillsammans den samlade bilden av vilken grad av tillit som kan sättas till en identitetsutfärdare. Apotekens Service anser att dessa tre delar väger lika tungt i bedömningen av den totala tillitsnivån.



¹ Återstår att definiera

5.1 Attributsutfärdare

Utvärderingskriterierna för attributsutfärdare är i huvudsak de samma som för identitetsutfärdare med följande huvudsakliga skillnader:

- Attributsutfärdare ställer ut attribut på grundval av att en autentisering och identifikation redan skett gentemot tjänsteleverantören, samt att ett intyg för denna autentisering och identifikation kan uppvisas.
- Attributsutfärdare ansvarar för länkningen mellan attribut och uppvisade identiteter. Attribut får inte under några omständigheter utfärdas utan att identiteten ifråga är knuten till ett givet attributvärde i attributsutfärdarens attributregister.
- Attributsutfärdare ansvarar för alla kvalitetsaspekter i hantering och lagring av attribut i enlighet med de regler som tillämpas för den/de federationer som attributsutfärdaren verkar inom.

6 Exempel på relationen mellan olika utvärderingskriterier

Nedanstående förenklade tabeller visar två exempel på Apotekens Service tolkning av hur olika nyanser av utvärderingskriterier tillsammans ger den samlade bilden av tillitsnivå.

Exempel där kraftfulla processer kompenserar för en svagare identitetsbärare:

Exempel på utvärderingskriterier	Resultat av utvärdering (låg, medium eller hög nivå)
Identitetsbärare	Medium
Livscykelhantering av identiteter	Hög
Operationella rutiner för identitetsutfärdare	Hög
Tekniska skyddsåtgärder för identitetsutfärdare	Hög
Summa tillitsnivå	Tillitsnivå tre

Exempel där svag livscykelhantering av identiteter medför en lägre tillitsnivå trots att en stark identitetsbärare används.

Exempel på utvärderingskriterier	Resultat av utvärdering (låg, medium eller hög nivå)
Identitetsbärare	Hög
Livscykelhantering av identiteter	Låg
Operationella rutiner för identitetsutfärdare	Medium
Tekniska skyddsåtgärder för identitetsutfärdare	Hög
Summa tillitsnivå	Tillitsnivå två

7 Sammanfattning av tillitsnivåer och exempel på användningsområden

Följande tabell sammanfattar de tre första tillitsnivåerna och visar exempel på autentiseringsmetoder för respektive nivå.

Tillitsnivå	Exempel	Utvärdering av brukarorganisation	Utvärdering av identitets-hantering	Autentiserings-metoder
1	Åtkomst till publik information.	Minimal utvärdering av brukarorganisation.	Minimal utvärdering, självregistrerade identiteter.	<ul style="list-style-type: none"> Ingen autentisering Användarnamn/lösenord PIN-kod
2	Åtkomst till intern information.*	Viss utvärdering av brukarorganisation.	Viss utvärdering, redovisning av identitetshantering.	<ul style="list-style-type: none"> Användarnamn/lösenord Kryptografiska hård- och mjukvaruenheter samt engångstokens med begränsad livscykelhantering
3	Åtkomst till konfidentiell information	Stringent och återkommande utvärdering av brukarorganisation.	Stringent och återkommande utvärdering av identitetshantering.	<ul style="list-style-type: none"> Kryptografiska hård- och mjukvaruenheter samt engångstokens med starkt kontrollerad livscykelhantering
4	Tillämpas ej	Tillämpas ej	Tillämpas ej	Tillämpas ej

* - En av Apotekens Service informationsklasser. Intern information definieras som information avsedd för arbetsrelaterat och internt bruk inom Apotekens Service AB eller som en del i en affärsrelation med leverantörer eller aktörer. Affärsavtal eller sekretessförbindelse måste finnas mellan Apotekens Service AB och annan organisation innan information av denna typ lämnas ut.

8 Bilaga 1 – Exempel på utvärderingskriterier för tillitsnivå tre²

För en komplett bild av ramverket, se <http://kantarainitiative.org/>

8.1 Administrativa krav

Identitetsutfärdare skall kunna:

- Redovisa dokumenterade regler, rutiner och organisation för all form av livscykelhantering av identiteter, t ex.
 - Hur ansökan går till
 - Hur identitetskontroll av den som ansöker sker
 - Hur utfärdandet går till
 - Hur en identitet kan spärras
 - Hur förnyelse av en identitet går till
 - Hur identiteter tilldelas egenskaper
 - Hur identiteter hålls unika vid registrering samt över/efter dess livslängd
 - Observera att inga former av självregistrering av identitetsuppgifter tillåts för tillitsnivå tre, samtliga identitetsuppgifter skall tilldelas identitetsinnehavaren genom fastslagna regler och rutiner.
- Utföra identifiering av identitetsinnehavare via personlig närvaro samt legitimera dessa vid utkvittering av identitet med en erkänd och accepterad legitimation, vilket exempelvis kan inkludera:
 - SiS märkt ID-kort
 - Nationellt ID-kort, utfärdat av svensk polis
 - Svenskt körkort
 - Svenskt EU-pass
 - ID-kort utfärdat av Skatteverket
 - Nationellt ID-kort utfärdat i annat EU-land samt Norge, Island, Liechtenstein och Schweiz
 - Utländskt EU-pass. Pass från Bulgarien, Cypern och Rumänien räknas inte som EU-pass
 - Utländskt inplastat körkort utfärdat inom EU samt Norge, Island och Liechtenstein
 - Utländskt pass, utanför EU
- Identitetsutfärdare skall tillämpa möjligheter för identitetsinnehavare att kunna spärra sin egen identitet i de fall identitetsinnehavaren misstänker eller kan konstatera identitetsstöld eller förvanskning.
- Redovisa vilken information som loggas och/eller arkiveras av identitetsintygsutfärdare vid utfärdande av identitetsintyg.

² OBS! Apotekens Service egen översättning från engelska.

- Redovisa hur identitetsintygsutfärdares logguppgifter skyddas samt hur länge uppgifterna lagras.
- Redovisa eventuella restriktioner för tjänsteleverantörer att logga åtkomst och identitetsintyg enligt sina regler och rutiner.
- Identitetsutfärdare skall hålla identitetsintygsutställare tillgängliga i enlighet med det/de avtal som tecknas med den/de federation(er) som identitetsutfärdaren verkar inom.
- Vid planerade avbrott i identitetsintygsutställares tillgänglighet skall tjänsteleverantörer notifieras med en god och i förväg redovisad framförhållning.
- Redovisa administrativ organisation och administrativa regler som appliceras på identitetsutfärdare.
- Identitetsutfärdaren skall tillsätta en supportorganisation i enlighet med de regler och avtal som finns för den/de federation(er) som den verkar inom.
- Identitetsutfärdare skall utan fördröjning informera tjänsteleverantörer om egna identitetsintygsutfärdarsystem eller dess informationskällor blivit utsatta för olaga intrång eller på annat sätt komprometterats. Säkerhetsincidenter skall hanteras i enlighet med de regler som den/de federationer identitetsutfärdaren verkar inom medför.
- Identitetsutfärdaren skall utse minst en ansvarig kontaktperson som ansvarar för information till tjänsteleverantörer samt berörda federationsägare för utbyte av information.
- Redovisa ansvarsfördelningen mellan identitetsintygsutfärdare och identitetsinnehavare. En identitetsinnehavares ansvar vid alla former av normalt bruk samt onormala situationer såsom stöld av identitetsbärare skall redovisas av identitetsutfärdaren.
- Redovisa eventuella restriktioner för nyttjande av utfärdade identitetsintyg.
- Redovisa vilka krav och eventuella avgifter identitetsutfärdaren applicerar på tjänsteleverantörer. De krav som identitetsutfärdaren eventuellt ställer på tjänsteleverantörer skall tydligt redovisas för att tjänsteleverantörer skall erkänna dessa krav och kunna ta ställning till dem.
- Löpande redovisa vilken/vilka identitetsfederation(er) identitetsutfärdaren verkar inom. Om en identitetsutfärdare verkar inom en eller flera identitetsfederationer skall detta redovisas tillsammans med den eller de federationspolicys som appliceras på identitetsutfärdaren.
- Löpande redovisa vilket/vilka tillitsramverk som appliceras på identitetsintygsutfärdare samt enligt vilken tillitsnivå. För att tjänsteleverantörer skall kunna acceptera en identitetsutfärdare måste dessa tillitsramverk möta upp till de krav som tjänsteleverantörer tillämpar.

- Periodiskt, samt vid begäran, utöva tillsyn och revision för att identifiera eventuella avsteg från den tillitsnivå identitetsutfärdaren tillämpar. Sådan revision och tillsyn skall ske i enlighet med de regler som finns uppsatta för den/de federation(er) som identitetsutfärdaren verkar inom.

8.2 Krav på handhavande (Operationella krav)

- Redovisa operationella processer och rutiner som används för att drift och underhåll av identitetsintygsutfärdare. Exempelvis hur konfigurationsförändringar godkänns och dokumenteras eller hur backuper hanteras.
- Redovisa fysiska och logiska skyddsåtgärder som tillämpas av identitetsutfärdare. Detta skall redovisas i form av skyddsåtgärder som implementeras från identitetsutfärdarens kontrollkatalog knuten till dess ledningssystem för informationssäkerhet.
- Redovisa rutiner och regler för hantering av situation där identitetsintygsutfärdare komprometterats. Exempelvis då identitetsintygsutfärdarens privata nyckel/nycklar blivit stulna eller förvanskats.
- Redovisa avvecklings-, förnyelse- och ersättningsplaner för identitetsintygsutfärdare.
- Redovisa giltighetstider på utställda identitetsintyg från identitetsintygsutfärdare.

8.3 Tekniska krav

- Identitetsintygsutfärdare skall ställa ut identitets- och attributintyg som följer OASIS SAML v2-specifikationer.
- Identitetsintygsutfärdare skall vara kompatibla med SAML 2.0 Authentication Request Protocol vid förfrågan om intyg.
- Identitetsutfärdare skall publicera korrekt och aktuellt SAML metadata för den/de identitetsintygsutfärdare man ansvarar för. Observera att detta även gäller tjänsteleverantörer och dessas "Service Providers".
- Identitetsutfärdare skall förbinda sig att löpande upprätthålla hög teknisk kvalitet och säkerhetsnivå för den/de identitetsintygsutfärdare man ansvarar för. Detta inkluderar exempelvis att tillämpa säker hård- och mjukvarukonfiguration samt att hantera regelbundna säkerhetsuppdateringar och härdning av den/de identitetsintygsutfärdare man ansvarar för.
- Använda sig av IDP-certifikat för signering och identifikation från, av federationsägaren godkända, CA:s.
- Utfärda de attribut som tjänsteleverantörer kräver i identitets- och attributintyg.
- Globalt registrera SAML-attribut som utfärdas via identitets- och attributintyg.
- Redovisa skydd av identitetsintygsutfärdarens privata nycklar för signering och identifikation, detta skydd skall godkännas av federationens ägare.

- Tillämpa kryptografiska mönster, algoritmer och nycklar i enlighet med de krav som federationens ägare ställer på identitetsleverantörer. Observera att detta även gäller tjänsteleverantörer och dessas "Service Providers".
- Identiteter skall skyddas av multifaktorsautentisering som godkänns av federationens ägare för respektive tillitsnivå. För tillitsnivå tre kan detta exempelvis implementeras i form av:
 - Certifikat och nycklar lagrade på kryptografisk enhet certifierad enligt FIPS 140-2 level 2.
 - Användarnamn+lösenord+engångskod (hanterad via separat autentiseringskanal såsom via en godkänd kodgenerator eller engångskod via SMS till ett på förhand registrerat SIM-kort).
- Samtliga typer av identitetsbärare skall tillämpa en låsmekanism vid X antal misslyckade inloggnings/upplåsningsförsök.
- Identitetsintygutfärdare skall implementera ett eller flera, av federationsägaren, godkända autentiseringsprotokoll som används vid autentisering av den/de part(er) som försöker kvittera ut identitetsintyg.
- Transportprotokoll mellan användare, identitetsintygutfärdare samt tjänstegränssnitt skall skyddas av en, av federationsägaren, godkänd kryptografisk lösning.

9 Bilaga 2 – Exempel på olika former av autentiseringsmetoder i olika tillitsnivåer

Nedan följer några exempel på hur olika typer av produktifierade identifikationsmetoder kan appliceras för de olika tillitsnivåerna.

Tabellen nedan visar de identifikationsmetoder som Apotekens Service valt att tillämpa.

Tillitsnivå	Exempel på tokentyper	SAML-authentication context
1	Ingen token	urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword
	Användarvalt lösenord	urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorUnregistered
	Användartilldelad säkerhetskod	urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorUnregistered
	MIFARE Classic token	urn:oasis:names:tc:SAML:2.0:ac:classes:MobileOneFactorContract
		urn:oasis:names:tc:SAML:2.0:ac:classes>Password
		urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard *

* - Får endast appliceras på nyttjande av ISO/IEC 14443 Type A 13,56 MHz contactless smart card standard

Tillitsnivå	Exempel på tokentyper	SAML-authentication context
2	Användarnamn/lösenord hanterade enligt regler och rutiner för tillitsnivå 2.	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
3	SITHS HCC_Person och HCC_Funktion Telia e-legitimation Mjuka certifikat** Engångskodslösningar i enlighet med tillitsnivå tre, exempelvis: <ul style="list-style-type: none"> • SMS-token • Kodgenerator-token 	urn:oasis:names:tc:SAML:2.0:ac:classes:SoftwarePKI urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI urn:oasis:names:tc:SAML:2.0:ac:classes:MobileTwoFactorContract urn:oasis:names:tc:SAML:2.0:ac:classes:Token ***
4	N/A	N/A

** - Denna typ av identitetsbärare ligger på tillitsnivå tre enligt Kantara Identity Assurance Framework

*** - Detta SAML authentication context ingår ej i OASIS SAML v2-specifikationerna men används av vissa kommersiella IDP-produkter som autentiserar användare med engångslösenord. Bör brukas återhållsamt för att istället fokusera på de authentication context som ingår i OASIS SAML v2-specifikationerna.

Not!

Följande SAML authentication context, dvs identifikationsmetoder, som medföljer OASIS SAML v2 har utgått:

- Timesync
- InternetProtocol
- Unspecified
- XML-signature
- Samtliga telephonyrelaterade context

Anledningen till att ovanstående utgått är att Apotekens Service bedömer dessa som ej tillämpbara.

Observera att det även finns ett SAML authentication context vid namn PreviousSession . Apotekens Service godkänner inte PreviousSession som authentication context vid en initial identifikation vid utkvittens av identitetsintyg.

10 Revisionshistorik

Utgåva	Datum	Kommentar
V 1.0	2011-12-12	Första utgåvan