apotekens service

Säkerhetskrav på extern part

som ansluter till Apotekens Service AB:s IT-tjänster

Innehåll

1 Inledning

Detta dokument beskriver Apotekens Service AB:s säkerhetskrav på aktörer som ansluter sig till Apotekens Service AB:s IT-tjänster.

2 Allmän information

Apotekens Service har för avsikt att anpassa sin säkerhetsarkitektur och därmed åtkomst till erbjudna tjänster i enlighet med de krav och regler som E-legitimationsnämnden specificerar inom ramen för Infrastrukturen för Svensk e-legitimation.

3 Regulatoriska krav

Krav S1: Aktör som ansluter till och utnyttjar Apotekens Service tjänster skall känna till och leva upp till gällande regulatoriska krav som tjänsterna omfattas av. Aktören skall ha nödvändiga processer, metoder och verktyg på plats som garanterar detta.

Exempel på lagar som gäller för Apotekens Service och de register och tjänster som tillhandahålls:

- Lagen (1996:1156) om receptregister
- Lagen (2005:258) om läkemedelsförteckning
- Lagen (1998:204) om personuppgifter

Notera: För apoteks- och vårdaktörer gäller även andra lagar, t ex apoteksdatalagen och patientdatalagen

Krav S2: Aktörer som ansluter till och använder Apotekens Service AB:s tjänster skall följa tillsynsmyndighetens, dvs Datainspektionens, råd och föreskrifter.

4 Säkerhetskrav

4.1 Anslutning via tjänstegränssnitt

Krav S3: Aktörerna skall ansluta sig till Apotekens Service AB:s IT-tjänster via de tjänstegränssnitt som Apotekens Service tillhandahåller och enligt de gällande regler som Apotekens Service specificerar .

4.2 Skydd mot skadlig kod

Krav S4: Aktören skall se till att endast datatrafik ämnad för Apotekens Service (behörig datatrafik) kommuniceras över Sjunet, Internet eller annan Partnerförbindelse till Apotekens Services system. Aktören skall se till att skydd mot skadligt intrång och skadlig kod är implementerat.

4.3 Autentisering och auktorisation

Aktören skall säkerställa att medarbetare är både identifierade och har korrekt behörighet vid utnyttjande av Apotekens Service tjänster.

Krav S5: Minst tvåfaktorsautentisering skall användas vid åtkomst till känslig information, t ex personuppgifter.*

Krav S6: Endast unika och personliga användaridentiteter får användas
Det inte är tillåtet att en person loggar in med exempelvis olika gruppkonton eller andra gemensamma roller/identiteter.

*) ***Information:***
Grunden för vilken autentiseringsmetod som tillämpas när en användare legitimerar sig är den tillitsnivå som tjänsten kräver. För åtkomst till information där det går att se substantiella konsekvenser vid en felaktig identifiering, t ex i fallet med åtkomst till personuppgifter, har Apotekens Service för avsikt att anpassa sig till kraven för tillitsnivå 3 (AL3). Se vidare kommande standard ISO 29115 samt Kantara IAF ” Initiative Identity Assurance Framework

4.4 Spårbarhet

Krav S7: Skall implementeras i enlighet med lagkrav på loggning för stickprovskontroll.
I händelse misstanke om obehörig åtkomst, t ex vid en incident eller i samband med Apotekens Service stickprovskontroll, skall aktör kunna avgöra om åtkomsten varit befogad eller ej.

4.5 Kryptering av informationsväxling

Krav S8: Information med känsligt innehåll (t ex personuppgifter) som via någon form av elektroniskt medium kommuniceras med Apotekens Service AB, skall krypteras, antingen symmetriskt eller asymmetriskt.

Val och införande av krypteringsmetod skall ske i samråd med Apotekens Service.

Rekommendation:
Symmetrisk kryptering: Minst 256 bitars nyckelängd
Asymmetrisk kryptering: Minst 1024 bitars nyckellängd

Revisionshistorik

Utgåva	Datum	Kommentar
1.0	-	-
2.0	2009-09-30	Uppdaterad
3.0	2011-03-08	Granskad av Manne Andersson , Gunnel Bridell, Maria Wettermark och ext-Patrik Thörnblad och ext- Conny Balazs