Riktlinje för tillhandahållande av behörighetsstyrande attribut

Ver 0.1

Innehåll

1. Inledning

För åtkomst till E-hälsomyndighetens register ställs höga krav på tillit till elektroniska identiteter som begär åtkomst och till behörighetsgrundande information och attribut kopplat till dessa identiteter.

2. Syfte

Syftet är att beskriva grundläggande säkerhetsnivå som E-hälsomyndigheten ställer på tillhandahållare av behörighetsstyrande attribut och som används vid åtkomstbegäran till myndighetens produkter och tjänster.

3. Omfattning

Anvisningar i denna riktlinje omfattar part som tillhandahåller behörighetsstyrande attribut kopplade till elektroniska identiteter vars hantering regleras genom Sweden Connect[1] och som nyttjas för åtkomst till myndighetens register.

4. Avgränsning

Part som tillhandahåller behörighetsstyrande attribut kopplade till elektroniska identiteter som nyttjas för åtkomst och vars hantering regleras genom SAMBI[2] och dess tillitsramverk, omfattas inte av denna riktlinje.

5. Termer och begrepp

Allvarlig säkerhetsincident: *Rapporteringspliktig säkerhetsincident* som kan komma att föranleda omedelbara åtgärder bland de parter som förlitar sig på tillhandahållna tjänster.

Användarorganisation: Organisation som bedriver verksamhet inom hälso- och sjukvården inkluderat vård av djur och djurhälsa, omsorgen eller som öppenvårdsapotek.

Attribut: Egenskap hos en medarbetare vid en *Användarorganisation* som ligger till grund för beslut om *Åtkomstkontroll* i en ansluten *E-tjänst* eller *Bastjänst*.

[1] https://swedenconnect.se/
[2] https://www.sambi.se/

Attributintyg: Ett intyg i elektronisk form av urkundskvalitet utställt av *Tillhandahållare av behörighetsstyrande attribut* som innehåller *Attribut* knutna till en viss person

Attributkälla: Register innehållande kvalitetssäkrade *Attribut* kopplade till en elektronisk identitet.

Attributprofil: Specifikation som beskriver förekommande *Attribut* och deras innebörd, och som bygger på sektorgemensamma överenskommelser med berörda parter.

Autentisering: Verifiering av en påstådd elektronisk identitet.

Behörighet: Tilldelade rättigheter att använda en informationstillgång på ett specificerat sätt.

E-legitimation: En elektronisk identitetshandling innehållande uppgifter som entydigt kan kopplas till en viss person och som kan användas för att identifiera innehavaren på elektronisk väg.

E-tjänst: Informationstjänst med användargränssnitt som baserat på *Identitetsintyg* medger att medarbetare vid en *Användarorganisation* bereds åtkomst till tjänsten och eventuellt bakomliggande *Bastjänster*.

Rapporteringspliktig säkerhetsincident: En oönskad och oplanerad händelse som kunnat ha eller haft påverkan på säkerhetsskyddet omgärdande en tillhandhållen tjänst, eller som kunnat innebära eller inneburit en störning i tillhandahållarens förmåga att fullgöra de åtaganden som följer av tecknade avtal.

Självdeklaration: En försäkran upprättad av *Leverantör av identitetintyg* eller *Federationsoperatör* som beskriver hur krav i respektive regelverk efterlevs.

Tillhandahållare av behörighetsstyrande attribut: Tjänst som omfattar *Attributkälla* och som förmedlar sådana kvalitetssäkrade uppgifter i formen av *Attribut* till leverantör av *E-tjänst*.

Åtkomstkontroll: Styrmedel i en *E-tjänst* som syftar till att reglera och begränsa en persons *Behörighet*.

6. Villkor om tillhandahållande av behörighetsstyrande attribut

Tillhandahållare av behörighetsstyrande attribut ska ställa upp nödvändiga villkor gentemot den Användarorganisation för vilken tillhandahållaren förmedlar behörighetsstyrande attribut till annan part.

Villkoren ska spegla de skyldigheter som åligger Användarorganisationen enligt denna riktlinje.

6.1 Informationssäkerhet

Tillhandahållare av behörighetsstyrande attribut och dennes hantering av informationssäkerhet ska baseras på principer i enlighet med ISO/IEC 27001 eller motsvarande likvärdiga principer för ledning och styrning av informationssäkerhetsarbetet.

Tillitsgrundande är då tillhandahållare och dess ledning kan ge bevis på sitt åtagande att upprätta, införa, driva, övervaka, granska, underhålla och förbättra informationssäkerhetsarbetet och att processerna för varje steg är dokumenterade och planerade, samt att erforderliga resurser för genomförandet är tillsatta.

Tillhandahållares förmåga till ett strukturerat och riskbaserat arbete med informationssäkerhet kan styrkas genom certifiering av ackrediterad revisor. Om alternativa standarder eller principer tillämpas ska en analys av överensstämmelse mellan standarderna vara genomförd, för att klargöra att inga väsentliga avvikelser förekommer.

6.2 Riskhantering

Tillhandahållare av behörighetsstyrande attribut ska ha tydliga och samordnade arbetssätt inom ramen för riskhantering. Detta innebär en förmåga att identifiera, analysera och motverka risker i enlighet med fastställda processer och rutiner för riskhantering.

Processen för riskanalys ska vara dokumenterad och tillämpad för tjänsten, och ska bygga på en riskanalysmetodik som ger konsistenta, korrekta och jämförbara resultat. Processen ska innefatta att också utforma, införa och följa upp risklindrande åtgärder, samt utverkande av riskägarens godkännande av kvarvarande risk

Tillhandahållaren ska ha tydligt utpekade ansvarsroller såsom riskägare och åtgärdsägare samt kompetens att genomföra löpande riskanalyser i enlighet med tydliga metoder och värderingsmodeller.

Riskhantering ska ske kontinuerligt eller minst var tolfte månad.

6.3 Incidenthantering

Tillhandahållare av behörighetsstyrande attribut ska ha tydliga och samordnade arbetssätt inom ramen för incident- och avvikelsehantering med en hög medvetenhet och förmåga att upptäcka, hantera och utreda incidenter och avvikelser kopplade till tjänsten.

6.4 Incidentrapportering

Former för vidarerapportering och att lämpliga reaktiva och preventiva åtgärder vidtas för att lindra eller förhindra skada till följd en säkerhetsincident.

Vidarerapportering av allvarliga säkerhetsincidenter ska ske utan dröjsmål till berörda parter och innefatta alla uppgifter som finns tillgängliga och är relevanta för att dessa ska kunna vidta nödvändiga åtgärder för att hindra, begränsa eller lindra tänkbar skada. Så länge en sådan händelse är pågående ska förlitande parter kontinuerligt hållas underrättade om händelsen och dess förlopp.

Övriga Rapporteringspliktiga säkerhetsincidenter kan avrapporteras periodvis, dock med som längst kvartalsvisa intervall.

7. Tillhandahållande av behörighetsstyrande attribut

7.1 Tjänstens beskaffenhet

Utlämnande av Attribut ska föregås av en kontroll av den begärande parten. Attributintyg ska ha det format och följa den Attributprofil som från tid till annan krävs för åtkomst till de efterfrågade tjänsten och ska vara giltiga endast så länge som det krävs.

7.2 Villkor för underleverantörer

Tillhandahållare av behörighetsstyrande attribut som på annan part har lagt ut utförandet av en eller flera av de åtaganden som omfattas av denna riktlinje ska genom avtal definiera vilka av dessa åtaganden som underleverantören är ansvarig för och vilka krav som är tillämpliga på dem.

7.3 Hantering av behörighetsstyrande attribut

Informationsinnehållet i attributkällan ska vara korrekt och aktuellt. Där så är möjligt ska uppgifterna verifieras eller inhämtas och kontinuerligt uppdateras gentemot ursprungskällan såsom ett officiellt register. Som sådan källa räknas till exempel Skatteverkets folkbokföringsregister, Socialstyrelsens register över legitimerad hälso- och sjukvårdspersonal (HoSP), Inspektionen för vård och omsorgs (IVO) vårdgivarregister, Bolagsverkets näringslivsregister samt Statistiska Centralbyråns (SCB) register över offentliga organ.

Personer som registreras i attributkällan som medarbetare vid en Användarorganisation ska ha ett anställnings- eller uppdragsförhållande till den organisation de registreras under. Kontroller av att anställning- och uppdragsförhållanden består och att registrerade attribut är korrekta ska genomföras minst en gång per kvartal, såvida inte medarbetaren redan vid registreringen har ett starkt tidsbegränsat uppdrag (mindre än 6 månader) och där behörigheten på förhand begränsats på samma sätt.

Rutiner för registrering, uppföljning, ändring och avregistrering av uppgifter i attributkällan ska vara dokumenterade, beslutade och tillämpade. Rutinerna ska innefatta att utan dröjsmål avregistrera sådana attribut som inte längre är aktuella då en person avslutar sin anställning eller sitt uppdrag, eller får ändrade arbetsuppgifter.

7.4 Styrning av åtkomst

Vid åtkomst av administrativ karaktär till Attributkälla och andra för säkerheten kritiska systemkomponenter ska strikt åtkomstkontroll tillämpas. Med detta avses att individuella och personbundna Behörigheter ska nyttjas i kombination med stark Autentisering av administratörens identitet.

7.5 Tekniska och kryptografiska säkerhetsåtgärder

Tekniska styrmedel och kontroller ska finnas införda som är tillräckliga för att säkerställa integritet, sekretesskydd, tillgänglighet och spårbarhet i de system och i den information som systemen behandlar. Med detta avses att tillhandahållare ska vidta de skyddsåtgärder som bör anses lämpliga och tillräckliga med beaktande av tillgänglig teknik, kostnaden för genomförandet av åtgärderna och de uppsatta riskacceptanskriterierna.

Principer som bör tillämpas är djupledsförsvar och överlappande säkerhetsåtgärder. Detta innefattar bland annat krypteringsåtgärder, styrmedel för nätverkskommunikation i flera nivåer och restriktiv åtkomstkontroll till systemresurser och informationstillgångar.

Känsligt kryptografiskt nyckelmaterial som används för att identifiera kommunicerande parter vid överföring och utväxling av säkerhetskänsliga uppgifter ska skyddas så att åtkomst begränsas, logiskt och fysiskt, till de roller och de tillämpningar som oundgängligen kräver det.

Kontrollernas effektivitet och tillräcklighet ska regelbundet utvärderas som del i kontinuerliga förbättringsarbetet.

7.6 Fysisk, administrativ och personorienterad säkerhet

De systemkomponenter som attributkällan byggs upp av ska skyddas fysiskt mot skada som följd av otillåten åtkomst eller andra yttre störningar. Tillträdeskontroll till dessa skyddade utrymmen ska tillämpas så att åtkomst till den tekniska och fysiska omgivning där tjänsten finns installerad begränsas till de personer vars arbetsuppgifter kräver det.

Personal som deltar i verksamheten och som är av särskild betydelse för säkerheten ska ha genomgått bakgrundskontroll. Detta i syfte att förvissa sig om att personen kan anses vara pålitlig samt att personerna har de kvalifikationer som krävs för att på ett tillfredsställande, korrekt och säkert sätt utföra sina arbetsuppgifter.

7.7 Spårbarhet

Samtliga administrativa åtgärder och förändringar i attributkällan ska kunna spåras genom en behandlingshistorik (logg) på individnivå.

Tiden för uppgifternas bevarande ska inte understiga fem år och uppgifterna ska kunna tas fram i läsbar form under hela denna tid, såvida inte krav på gallring påkallas från integritetssynpunkt och har stöd i lag eller annan författning.

8. Internkontroll

Tillhandahållare av behörighetsstyrande attribut ska inrätta en funktion för internrevision som periodiskt granskar verksamheten och efterlevnaden av ställda krav. Internrevisorn ska självständigt planera genomförandet av revisionen och dokumentera detta i en revisionsplan. Revisionsmoment ska väljas utifrån en risk- och väsentlighetsanalys och grundas i den självdeklaration som tillhandahållaren lämnat.

Internrevisorn ska vara oberoende i utförandet av uppdraget på ett sätt som tryggar en objektiv och opartisk granskning. Internrevisorn ska också ha den kompetens och erfarenhet som krävs för att med rimlig säkerhet kunna påvisa att den försäkran som lämnats genom självdeklarationen, från tid till annan, inte är behäftad väsentliga fel. En sådan grad av säkerhet anses kräva viss insamling och verifiering av objektiva bevis.

Resultatet av internrevisionen ska dokumenteras i en internrevisionsrapport och innefatta ett uttalande om internrevisionen anser att lämnade beskrivningar i självdeklaration återspeglar en rättvisande bild av hur kraven i regelverket uppfylls eller om självdeklarationen kan vara behäftad med väsentliga felaktigheter.

9. Självdeklaration

Tillhandahållare av behörighetsstyrande attribut ska upprätta en försäkran som beskriver hur grundläggande säkerhetsnivå angivet i denna riktlinje är uppnådd.

Försäkran innebär en självdeklaration av samtliga områden inför ett godkännande. Förnyad självdeklaration ska genomföras senast vart annat år efter godkännande eller vid större förändringar kopplat till tjänsten.

Dokumentinformation

Dokumentnamn Riktlinje tillhandahållande av behörighetsstyrande attribut		**Diarienr**
Beslutad av (Namn, Befattning, Avdelning) Stephen Dorch, Säkerhetsskyddschef, Stab		
Dokumentansvarig (Namn, Avdelning, Enhet) Richard Åström Einarsson, Stab, Verksamhetsledningssystem		
Beslutsdatum 2021-xx-xx	**Ikraftträdandedatum** 2021-xx-xx	**Gäller t.o.m.** Tills vidare
Informationssäkerhetsklass Öppen	**Lagrum**	

Versionshistorik

Utgåva	Datum	Kommentar
0.1	2021-05-26	Utkast

Hänvisning till externa krav som föranlett styrdokumentet

Lag (2018:1212) om nationell läkemedelslista
MSBFS 2020:6 Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet
MSBFS 2020:7 Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter
EU:s dataskyddsförordning (EU) 2016/679