Granskning av hantering av e-tjänstekort

Rapport

Region Dalarna

KPMG AB

2023-11-13

Antal sidor 23

Region Dalarna
Granskning av hantering av e-tjänstekort

2023-11-13

Innehållsförteckning

1 Sammanfattning

KPMG har av Region Dalarnas revisorer fått i uppdrag att granska rutinerna kring regionens hantering av e-tjänstekort. Uppdraget ingår i revisionsplanen för år 2023.

Syftet med granskningen har varit att bedöma om Region Dalarna säkerställt en tillräckligt säker hantering av certifikat för använda e-tjänstekort.

Vår sammanfattande bedömning utifrån granskningens syfte är att regionstyrelsen inte säkerställer en tillräckligt säker hantering av e-tjänstekort i Region Dalarna utifrån sitt övergripande ansvar för säkerheten i regionen.

Vi bedömer därtill att hälso- och sjukvårdsnämnden i egenskap av vårdgivare inte säkerställer tillräcklig intern kontroll över de processer som enligt gällande lagstiftning ska garantera informationssäkerhet, patientsäkerhet och sekretess.

Det finns i allt väsentligt dokumenterade rutiner för hantering av e-tjänstekort och regionens regler avseende åtkomst och behörighet. Vi bedömer dock att efterlevnaden av rutinerna är bristfällig vilket leder till att nuvarande behörighetstilldelning och/eller avslut som vi i granskningen kan påvisa medför risker i spårbarhet för åtkomst till information och lokaler.

Granskningen visar att det finns betydande risker kopplat till vissa typer av kort som inte är spårbara och som kräver manuell hantering och kontroll. Vi konstaterar därtill att det förekommer alltför generösa behörigheter i förhållande till vad som behövs för att den enskilde ska kunna utföra sitt arbete. Bakgrunden till ovan är bristfällig efterlevnad till de rutiner som finns, samt bristfälliga manuella och systemtekniska kontroller. Vi bedömer således att hälso- och sjukvårdsnämndens verksamheter idag inte uppfyller patientdatalagens krav om att behörighet ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Detta bedömer vi som allvarligt beaktat kraven i lagstiftningen, men också utifrån att det innebär bristande efterlevnad till Region Dalarnas informationssäkerhets- och dataskyddspolicy.

Ovan beskrivna brister beror enligt vår mening till stor del på att det saknas ett uttalat ansvar för helheten och processen som hantering av e-tjänstekort, certifikat och åtkomst och behörighet består av. I nuläget saknas därigenom en övergripande bild över risker och brister. Styrningen från central nivå har förskjutits, å ena sidan till verksamheterna att själva ta ansvar för att hanteringen av tjänstekorten fungerar och följs upp och å andra sidan till regionstyrelsens förvaltning som hanterar den praktiska delen genom kortkontorens tillhandahållande. Vi bedömer att det saknas dokumentation om rapporteringsansvar och ansvar för samordning vilket innebär att det inte finns någon uttalad aktör med övergripande ansvar för informationssäkerheten och den fysiska säkerheten vad gäller kort- och certifikatshanteringen.

På följande sida redovisas våra bedömningar och rekommendationer kopplat till revisionsfrågorna.

Revisionsfråga	Bedömning: I allt väsentligt	Rekommendationer
Är det tydligt vilka personer i organisationen som har rättighet att besluta om tilldelning av olika certifikat?	Ansvar finns tydliggjort i styrande dokument samt i detaljerade rutinbeskrivningar och efterlevs i vår mening i allt väsentligt. Vi ser dock behov av att tydliggöra var det övergripande ansvaret i regionen finns för uppföljning och kontroll av processen för e-tjänstekort och certifikat.	**Vi rekommenderar regionstyrelsen** att: - I sitt övergripande ansvar tillse en utvecklad samordning av regionens arbete för att skapa en tydligare ansvars-fördelning för hantering av e-tjänstekort och certifikat. - Komplettera styrande dokument med tydliggörande av hur uppföljning av den övergripande hanteringen av e-tjänstekort, åtkomst och behörighet ska göras samt vem som ansvarar för denna.
Revisionsfråga	**Bedömning: Delvis**	**Rekommendationer**
Säkerställer kortkontorets interna rutiner en trygg och ändamålsenlig hantering av certifikat? • **Är kontrollen av att beslut om att tilldela certifikat fattats av behörig personal tillräcklig?** • **Finns rutiner/system (spärrar, kontroller e t c) som säkerställer att certifikat inte läggs in felaktigt?**	Kortkontorets interna rutiner säkerställer en trygg och ändamålsenlig hantering av certifikat för anställda som erhåller tillsvidareanställning. Det finns betydande risker i nuvarande rutiner för icke spårbara kort med avsaknad av kontrollsystem, i det fall manuell hantering och kontroll brister. Det saknas tillräckliga rutiner eller system för att säkerställa att inte behörigheter till system och passage läggs in felaktigt. Vi konstaterar att nuvarande hantering i hög grad baseras på manuell hantering. Vi noterar att processerna och hanteringen är förenade med ett antal risker.	**Vi rekommenderar hälso- och sjukvårdsnämnden att:** - Säkerställa efterlevnad till den lagstiftning som reglerar elektronisk åtkomst och behörighet

Revisionsfråga	Bedömning: Nej	Rekommendationer
Är rutiner/system som ska säkerställa att tilldelade certifikat återkallas när personer till exempel lämnar sin anställning/uppdrag e t c ändamålsenliga och efterlevs, i förekommande fall, rutinerna?	Vi konstaterar att rutinen vid avslut av anställning är tydlig men inte alltid efterlevs. Vi bedömer att det finns rutiner som ska säkerställa att tilldelade certifikat behörigheter? återkallas när personer byter arbetsställe inom regionen men vi bedömer att efterlevnad till dessa är låg. Då det medför att medarbetare i kan inneha alltför generösa behörigheter bedömer vi som allvarligt beaktat kraven i lagstiftningen, men också utifrån att det innebär bristande efterlevnad till Region Dalarnas informationssäkerhets- och dataskyddspolicy.	**Vi rekommenderar hälso- och sjukvårdsnämnden att:** - Säkerställa att rutiner om avslut av anställning eller byte av arbetsställe är kända och efterlevs.
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Är rutinerna för hantering av certifikat vid långtidsfrånvaro e t c ändamålsenliga och efterlevs dessa?	Det saknas rutiner för hur e-tjänstekort, certifikat och tilldelade behörigheter ska hanteras vid långtidsfrånvaro eller annan längre frånvaro för anställda.	**Vi rekommenderar regionstyrelsen att:** - Säkerställa rutin samt kännedom om hantering av kort, certifikat och behörigheter vid långtidsfrånvaro. **Vi rekommenderar regionstyrelsen och hälso- och sjukvårdsnämnden att:** - I syfte att underlätta inventering av den totala mängden kort bör rutiner för detta införas samt, därtill genomföra regelbunden kontroll av inaktiva kort.

Revisionsfråga	Bedömning: Delvis	Rekommendationer
Har tillräckliga åtgärder vidtagits för att förhindra/försvåra att samma certifikat används av flera personer i organisationen (vid inloggning i olika system)?	Regionen har i information beskrivit hur kortet ska hanteras så som värdehandling. Utöver information har inga ytterligare åtgärder gjorts för att minimera eller kontrollera detta. Vi bedömer, mot bakgrund av de regelverk och tydliga lagkrav som styr verksamheten att det inte nog kan påtalas att varje enskild avvikelse åsidosätter såväl medarbetarens säkerhet som informationssäkerheten vilket innebär att avvikelser bör registreras och analyseras.	**Vi rekommenderar regionstyrelsen att:** - I högre grad beakta informationssäkerhetsrisker kopplat till åtkomst och behörighet givet ett förstärkt säkerhetsläge för cyberhot. **Vi rekommenderar hälso- och sjukvårdsnämnden att:** - Säkerställa medvetenhet om vikten av korrekt hantering av e-tjänstekort som värdehandling i syfte att riskminimera avvikelser avseende integritet, fysisk säkerhet och patientsäkerhet.
Revisionsfråga	**Bedömning: Nej**	**Rekommendationer**
Utgör dokumenterade riskanalyser underlag inför beslut om tilldelning till certifikat?	Vi uppfattar att behovs- och riskanalyser inte genomförs i enlighet med krav i Direktiv - Behovs- och riskanalys för behörighetstilldelning. Detta kan bero på att dokumenten inte är kända och etablerade i verksamheten.	**Vi rekommenderar regionstyrelsen och hälso- och sjukvårdsnämnden att:** - Säkerställa efterlevnad till den lagstiftning som reglerar elektronisk åtkomst och behörighet. **Vi rekommenderar hälso- och sjukvårdsnämnden att:** - Säkerställa aktualitet och giltighet för dokumentet Direktiv - Behovs- och riskanalys för behörighets-tilldelning samt tillkommande rutiner och tillse följsamhet till dessa.
Revisionsfråga	**Bedömning: Ja**	**Rekommendationer**
Har ansvariga förvissat sig om att användare har genomfört obligatoriska moment (utbildning mm.) innan de tilldelas åtkomst till information?	Vi bedömer att utbildning genomförs innan tilldelning av åtkomst till information. Vi ser därtill att ansvar för e-tjänstekort finns väl kommunicerat till medarbetare i syfte att tillse att dessa används korrekt.	Inga rekommendationer

2 Bakgrund

SITHS är en elektronisk identitetshandling som används för säker identifiering av både personer och system inom regioner, kommuner, privata vårdgivare och statliga myndigheter. Den elektroniska identitetshandlingen, e-tjänstekort, används till exempel vid inloggning i olika IT-baserade tjänster, för inpassering i lokaler o s v.

Alla anställda eller uppdragstagare i regionen ska ha ett e-tjänstekort. SITHS tillhandahålls och administreras av Inera AB. För att e-tjänstekorten ska fungera för inloggningar, inpassering e t c förses korten med ett s k certifikat som är en garant för att kortinnehavaren är anställd eller har uppdrag i Region Dalarna. Kopplat till kortets certifikat kan sedan behörigheter i passagesystem och informationssystem. Såväl tilldelning som avslut av certifikat och behörigheter baseras delvis på manuella rutiner. Hanteringen av certifikat sker för Region Dalarnas del av ett särskilt kortkontor men beslut om vilka behörigheter en anställd/uppdragstagare ska tilldelas fattas i linjeorganisationen.

E-tjänstekort finns av olika typer. I Region Dalarna används Företagskort (alla anställda med anställningstid över sex månader), Studentkort, Konsultkort och Reservkort (för personal med kortare anställningstid än sex månader). Certifikat går även att lägga på e-tjänstekort från till exempel en annan region.

Inera AB ställer höga krav på hanteringen av de elektroniska identitetshandlingarna varför revisorerna bedömer att utgivningen av e-tjänstekort i huvudsak är säkerställd. Däremot ser revisorerna att det finns avsevärda risker förenade med hanteringen av certifikat och även kring den praktiska användningen av e-tjänstekort i verksamheten.

Exempel på sådana risker kan vara att certifikaten inte upphör när en anställd/uppdragstagare lämnar regionen eller byter arbetsplats inom regionen eller att flera personer använder sig av samma behörighet, det vill säga att en person loggar in i ett system och att denna inloggning sedan används av ett flertal individer vilket försvårar spårbarheten i systemen.

2.1 Syfte, revisionsfrågor och avgränsning

Syftet med granskningen är att ge revisorerna underlag att bedöma om regionen säkerställt en tillräckligt säker hantering av certifikat för använda e-tjänstekort.

Granskningen ska bland annat lämna svar på följande frågeställningar:

- Är det tydligt vilka personer i organisationen som har rättighet att besluta om tilldelning av olika certifikat?
- Säkerställer kortkontorets interna rutiner en trygg och ändamålsenlig hantering av certifikat?
    - Är kontrollen av att beslut om att tilldela certifikat fattats av behörig personal tillräcklig?
    - Finns rutiner/system (spärrar, kontroller e t c) som säkerställer att certifikat inte läggs in felaktigt?

- Är rutiner/system som ska säkerställa att tilldelade certifikat återkallas när personer till exempel lämnar sin anställning/uppdrag e t c ändamålsenliga och efterlevs, i förekommande fall, rutinerna?
- Är rutinerna för hantering av certifikat vid långtidsfrånvaro e t c ändamålsenliga och efterlevs dessa?
- Har tillräckliga åtgärder vidtagits för att förhindra/försvåra att samma certifikat används av flera personer i organisationen (vid inloggning i olika system)?
- Utgör dokumenterade riskanalyser underlag inför beslut om tilldelning till certifikat?
- Har ansvariga förvissat sig om att användare har genomfört obligatoriska moment (utbildning mm.) innan de tilldelas åtkomst till information?

Avgränsning

E-tjänstekort används inom merparten av Region Dalarnas verksamheter och ingår i regionstyrelsens ansvarsområde. I syfte att avgränsa granskningen har ett antal intervjuer med verksamhetsföreträdare från hälso- och sjukvården genomförts vari det huvudsakliga antalet enskilda användare av e-tjänstekort finns.

Centrala begrepp

- **E-tjänstekort**: En elektronisk identitetshandling. E-tjänstekort används som elektronisk nyckel till lokaler och till vissa datasystem.
- **Certifikat**: Ett tjänstecertifikat laddas ned till kortet. Mjukvaran finns att tillgå via intranätet, och adderas till den elektroniska identitetshandlingen. E-tjänstekortet är bärare av giltigt certifikat. Ett funktionscertifikat finns i de system kräver kortet för att medarbetare ska kunna logga in.
- **Behörighet passage**: Åtkomst för passage till lokaler och utrymmen tilldelas genom behörigheter. Dessa baseras på medarbetarens organisationstillhörighet. Behörigheter till lokaler säkerställs genom att e-tjänstekort, reservkort eller nyckelkort förses med passagerättigheter.
- **Behörighet till informationssystem**: Åtkomst till informationssystem tilldelas genom behörigheter. Dessa baseras på medarbetarens roll och organisationstillhörighet. Vissa informationssystem som nyttjas i regionens verksamheter ställer krav om e-tjänstekort eller reservkort som en andra faktor vid inloggning utöver användarnamn och lösenord. Enligt uppgift beräknas Region Dalarna ha omkring 50 informationssystem där krav om SITHS-kort som andra faktor införts. Omkring 800 informationssystem har inte infört detta krav.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

- Kommunallag (2017:725) 6 kap. 6 §
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster

Lagen innebär i korthet att leverantörer av samhällsviktiga tjänster (exempelvis hälso- och sjukvård) ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster. Det ska finnas en riskanalys som ligger till grund för val av säkerhetsåtgärder och leverantören ska vidta ändamålsenliga tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten för att tillhandahålla samhällsviktiga tjänster. Vidare framgår att leverantörer av samhällsviktiga tjänster ska vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster.

- Patientdatalag (2008:355)

Lagen reglerar i huvudsak informationshantering inom hälso- och sjukvården. I lagen framgår att vårdgivare ska bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat. Sådan behörighet ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. Det omfattar även kontroll av elektronisk åtkomst, där vårdgivare ska göra systematiska och återkommande kontroller av om någon obehörigen kommer åt elektroniska patientdata uppgifter.

- Reglemente för regionstyrelsen, reglemente för hälso- och sjukvårdsnämnden[1]

  Av reglemente för **regionstyrelsen** framgår att styrelsen ska styra, utveckla och samordna förvaltningen av Region Dalarnas angelägenheter och utöva kontroll över övriga nämnders verksamhet. Det framgår vidare att styrelsen har det övergripande ansvaret för Region Dalarnas säkerhet som bl. a. omfattar patientsäkerhet, brandsäkerhet, IT-säkerhet och informationssäkerhet.

  Av reglementet för **hälso- och sjukvårdsnämnden** framgår bland annat att nämnden ska följa hälso- och sjukvårdslagen, patientsäkerhetslagen, patientdatalagen, patientlagen samt de övriga lagar och föreskrifter som gäller på hälso- och sjukvårdens område, samt, utifrån sitt uppdrag ska nämnden tillse att intern kontroll och uppföljning fungerar tillfredsställande.

- Övriga tillämpbara interna regelverk, policyer och beslut, till exempel informationssäkerhetspolicy och ledningssystem för informationssäkerhet

[1] RS 2023/767; HSN 2023/5646

2.3 Metod

Granskningen har genomförts genom:

— Dokumentstudier av för granskningen relevanta dokument.

— Intervjuer har genomförts med ett flertal tjänstepersoner med ansvar för säkerhet, informationssäkerhet, it, e-tjänstekort samt passage. Intervjuer har också genomförts med verksamhetschefer och första linjens chefer inom hälso- och sjukvården med ansvar för att tilldela behörigheter till medarbetare.

Samtliga intervjuade har erbjudits att faktagranska ett utkast av rapporten.

3 Resultat av granskningen

3.1 Ansvar och roller

Region Dalarna är anslutna till tjänsten SITHS som tillhandahålls av kommunernas och regionernas gemensamma digitaliseringsbolag Inera. SITHS är en elektronisk identitetshandling som används för säker identifiering av både personer och system. Samtliga organisationer som är anslutna till tjänsten har att förhålla sig till ett Tillitsramverk för SITHS[2] innehållandes reglering av de organisatoriska krav som ställs vid hantering av SITHS e-legitimation.

Den utfärdande organisationen ska, enligt tillitsramverket, upprätta ett utgivningsområde för utfärdande av e-tjänstekort. Kopplat till varje utgivningsområde ska finnas ansvarig utgivare, säkerhetsansvarig och en organisation med tillräcklig kapacitet för att sköta den praktiska hanteringen av e-tjänstekort.

3.1.1 Kortkontorets ansvar

Region Dalarna har upprättat ett utgivningsområde för utfärdande av e-tjänstekort som organisatoriskt tillhör regionstyrelsens förvaltning. Utgivningsområdet benämns kortkontoret.

Vi kan konstatera genom dokumentgranskning att Region Dalarnas interna organisationsbeskrivning för e-tjänstekort[3] med tillhörande funktionsansvar är samstämmigt med reglering i Ineras Tillitsramverk. Utöver de roller som Tillitsramverket ställer krav på har regionen en organisation för sin hantering av e-tjänstekort som består av biträdande ansvarig utgivare, ID-administratörer utfärdare och ID-administratörer handläggare. Administratörer och handläggare arbetar på uppdrag av kortkontoret men tillhör organisatoriskt respektive verksamhet där de är placerade. Det finns dokumenterad uppdragsbeskrivning[4] för ID-administratörer vilka beskriver befogenhet att utfärda och avsluta e-tjänstekort, passagekort samt passagerättigheter.

Av arbetsbeskrivning för säkerhetssamordnare[5] framgår att vederbörande ska tillse förutsättningar för en fungerande hantering av e-tjänstekort inom regionen. Enligt arbetsbeskrivningen avser det stöd och utbildning till administratörer av e-tjänstekort samt att tillse att processer för e-tjänstekort och passagebehörighet utgår från aktuella rutiner och riktlinjer. I funktionen för ansvarig utgivare och säkerhetsansvarig ingår till stor del kvalitetsarbetet avseende säkerhet och ledningssystem. Ansvarig utgivare är därtill skyldig att tillse att internrevisioner och riskanalys genomförs för utgivningsområdet.

Vi har i granskningen tagit del av genomförda internrevisioner men vi uppfattar att det i nuläget saknas riskanalyser för utgivningsområdet. En funktion inom hållbarhetsavdelningen genomförde 2022 en internrevision av e-tjänstekorthantering

[2] Tillitsramverk Identifieringstjänst SITHS, fastställd 2022-05-10
[3] Organisation e-tjänstekort Region Dalarna, fastställd 2019-02-06
[4] Uppdragsbeskrivning tillhörande avtal e-ID kort och passage mellan Säkerhet, risk och beredskap och Regionservice, daterad 2021-09-27
[5] Arbetsuppgifter säkerhetssamordnare, ej daterad

inom ledningsfunktionen (utgivningsområdet). Resultatet av internrevisionen var att kortkontoret hade systematiserade arbetssätt med grund i dokumenterade och aktuella rutiner. Däremot saknades instruktioner kring utlämning av e-tjänstekort på intranätet. Instruktioner och rutiner fanns däremot på säkerhet- och beredskapsenhetens interna lagringsyta, vilket ansågs alltför svåråtkomligt.

Intervjuade beskriver att kortkontorets ansvar, utöver det som är beskrivet ovan avseende utgivningsområdet, avgränsas till tillverkning och tillhandahållande av det fysiska kortet för e-legitimation. I ansvaret ingår att aktivera ett certifikat på kortet som intygar att innehavaren är anställd eller har uppdrag inom Region Dalarna. Detta certifikat agerar sedan ”nyckel” till andra behörigheter till system eller passage i fastigheter som kortinnehavaren ska ha åtkomst till, vilka läggs till efter beställning från behöriga chefer.

Hantering av ytterligare certifikat som medger åtkomst till system och lokaler tillhör inte kortkontorets ansvar och uppgifter.

3.1.2 Ansvar för åtkomst och behörighet

Styrande dokumenten som vi tagit del av beskriver organisation för och administrering av e-tjänstekort. De beskriver även ansvar som åvilar chefer respektive enskilda kortinnehavare i fråga om behörigheter och kortsäkerhet.

Riktlinjen för informationssäkerhet och dataskydd för beslutsfattare[6] reglerar ytterligare funktioner med ansvar för åtkomst och behörigheter.

- IT-direktör har övergripande ansvar för IT-säkerhetsarbetet med tillhörande IT-säkerhetskrav och beslutar därmed bland annat om rutiner och riktlinjer för tillträde till regionens datanät.
- HR-direktör ansvarar för processer inom identitets- och behörighetshantering.
- Verksamhetschef/enhetschef ansvarar för att besluta efter behovs- och riskanalys om behörigheter, att följa upp användaråtkomst till IT-stöd genom loggning samt att tillse att användare har erforderlig utbildning och kompetens före tilldelning av behörigheter.

Intervjuade beskriver att ansvar och hantering av åtkomst och behörighet är spritt mellan flertal funktioner och inte helt överblickbart i nuläget. Beställningar sker genom självbetjäningsportalen där endast behöriga har tillgång och kan besluta om nya, förändrade och avslut av behörigheter.

Systemförvaltare och/eller andra administrativa stödfunktioner inom respektive verksamhet kan ha delegerade arbetsuppgifter från verksamhetscheferna att praktiskt hantera tillägg, ändring och avslut av behörigheter efter att detta beställts av cheferna.

[6] Riktlinje Informationssäkerhet och dataskydd för beslutsfattare, godkänd 2022-04-04

3.1.3 Bedömning

Vi bedömer att det i allt väsentligt är tydligt vilka personer i organisationen som har rättighet att besluta om tilldelning av olika certifikat och att ansvaret följer reglering genom Ineras tillitsramverk och de av regionstyrelsen beslutade interna styrdokumenten inom informationssäkerhet.

Det finns därtill väl etablerade rutiner som beskriver på vilka grunder som e-tjänstekort och certifikat ska utfärdas och vem i organisationen som har rätt att göra detta.

Vi ser dock behov av att tydliggöra var det övergripande ansvaret i regionen finns för uppföljning och kontroll av processen för e-tjänstekort och certifikat. Ansvar i det praktiska utförandet är i stora delar decentraliserat till verksamheterna och fördelat på flertalet funktioner vilket i nuläget leder till att det saknas en övergripande och samlad bild över risker och avvikelser i processen.

Regionstyrelsen bör därför i sitt övergripande ansvar för Region Dalarnas patientsäkerhet, IT-säkerhet och informationssäkerhet tydliggöra detta ansvar så att det finns en tillräcklig intern kontroll över hanteringen av e-tjänstekort och certifikat på en aggregerad nivå.

3.2 Utfärdande av e-tjänstekort och tilldelning av certifikat

3.2.1 Övergripande krav

Enligt Tillitsramverket för SITHS ska utfärdande organisationer ha ett ledningssystem för informationssäkerhet. Region Dalarnas ledningssystem baseras på ISO27000-standarden och grunden är regionens Informationssäkerhets- och dataskyddspolicy[7].

Policyn anger bland annat att information endast får tillgängliggöras för behöriga användare samt att händelser i informationsarbetet ska vara spårbara. Till policyn är tre riktlinjer[8] kopplade, vilka redovisar ansvar för och hantering av informationstillgångar och informationssäkerhet inom regionen för användare, beslutsfattare respektive centrala stödfunktioner.

Riktlinjerna berör i delar reglering av e-tjänstekort där det framgår att behörigheter och e-tjänstekort är personliga och inte får lånas ut, samt beskrivning över hur korten ska hanteras ur säkerhets- respektive informationssäkerhetsaspekt.

Tillitsramverket redovisar regler, så kallade tillitsnivåer, som gäller för olika typer av e-tjänstekort. Reglerna korrelerar mot olika nivåer av behörigheter som kortinnehavaren via e-tjänstekortet får tillgång till och avser därför till exempel krav på identitetskontroll vid kortutlämning och giltighetstid för certifikat. Allmänna villkor för SITHS e-legitimation[9] redovisar de av Inera fastställda villkor som gäller för användare av e-

[7] Godkänd 2022-03-14
[8] Informationssäkerhet och dataskydd för användare, godkänd 2023-04-03, Informationssäkerhet och dataskydd för beslutsfattare, godkänd 2022-04-04, Informationssäkerhet och dataskydd för centrala stödfunktioner, godkänd 2023-04-04.
[9] Allmänna villkor för SITHS e-legitimation, daterad 2020-09-02

tjänstekort och utfärdande organisationer. Inera eller den utfärdande organisationen äger bland annat rätt att spärra kortet vid bekräftat eller misstänkt missbruk av kort eller koder samt om kortinnehavarens anställning upphör.

Inom Region Dalarna används fem olika typer av e-tjänstekort vilka finns beskrivna i bakgrundskapitlet (Kap. 2, s.6): Företagskort, Reservkort, Konsultkort, Studentkort samt Kort utfärdat av annan region/kommun. Vi noterar i granskningen att det finns motstridiga uppgifter gällande beskrivning av respektive korttyp och vilket kort som ska nyttjas utifrån målgrupp och kriterier. Korttyperna beskrivs dels i rutin för e-tjänstekort dels i information som presenteras i informationsbroschyr via intranätet[10]. Det material som erhålls via intranätet är uppdaterat under 2023 och genom den uppdateringen lättare tillgängligt för regionens medarbetare än tidigare.

3.2.2 Beställning och utlämning av e-tjänstekort (företagskort)

En grundläggande förutsättning för att kunna utfärda ett e-tjänstekort är att kortinnehavare måste ha en anställning inom organisationen, eller ha ett intygat uppdrag åt den organisation som ställer ut kortet. Vid anställning i Region Dalarna tilldelas medarbetaren en plats i den elektroniska katalogen, HSA-katalogen[11]. För utfärdare av e-tjänstekort framgår ansvar för att kortanvändarens angivna uppgifter kontrolleras mot folkbokföringsregistret via system som är godkända av Inera.

För administration och praktisk hantering kring utgivning av e-tjänstekort finns styrdokumentet Rutin för e-tjänstekort[12] som personal inom kortorganisationen utgår från. Vi konstaterar att rutinen på detaljerad nivå beskriver vilka moment som ska genomföras och av vem.

Av rutinen framgår att verksamhetschef, eller av verksamhetschef utsedd person, ansvarar för att beställa kortet. Beställningsförfarandet konkretiseras i ett informationsdokument riktat till chefer[13].

I intervju framförs att behörighetstilldelning ska baseras på organisationstillhörighet och anställningstyp, och att det är upp till den chef som beställer e-tjänstekortet att samtidigt beställa de behörigheter som anses nödvändiga.

I intervju med företrädare för Regionfastigheter framkommer att en viktig säkerhetsaspekt är att medarbetare finns tillagda på korrekt sätt i HSA-katalogen. En korrekt placering innebär att medarbetaren finns tillagd i den kategori som hen tillhör avseende såväl profession som fysisk placering. Behöver personen behörighet till annan verksamhet än den som följer med vederbörandes organisationstillhörighet ska en sådan ansökan godkännas av verksamhetschef för den verksamhet som behörigheten avser.

[10] Broschyr för e-ID kort, daterad 2023-06-09
[11] Inera webbplats: ”HSA är elektronisk katalog med kvalitetsgranskade uppgifter om organisationer och personer inom vård och omsorg i Sverige.”
[12] Rutiner e-tjänstekort Region Dalarna, senast reviderad 2021-01-20.
[13] Information för chefer, daterad 2021-11-12

Kännedom om att katalogbehörigheter fungerar på detta sätt samt följsamheten till gällande rutin uppges vara förhållandevis låg. Detta bedöms av den intervjuade vara en betydande säkerhetsrisk avseende åtkomst till fysiska lokaler.

Vi har tagit del av informationsbrev där säkerhetschef tydliggjort gällande rutiner för kort för passage[14]. Informationen tydliggör vikten av att hanteringen sker på ett korrekt sätt.

Efter att beställning av kortet och tillhörande passagerättigheter har gjorts adderas dessa av ansvarig utgivare, biträdande ansvarig utgivare eller kortadministratör, enligt rutinen för e-tjänstekort.

Vi får till oss att risker för att behörigheter läggs på av misstag, eller att kort utfärdas på felaktiga grunder, anses vara små då all hantering utgår från den kort- och behörighetsbeställning som chef genomför i Självbetjäningsportalen. Det sistnämnda beskrivs emellertid bidra till en omfattande administration för framför allt chefer inom vården där det finns en betydande andel personal med vikariat etcetera.

I samband med beställning av kort ansvarar rekryterande chef för att medarbetaren besöker ett av regionens fyra kortkontor[15] för fotografering. När e-tjänstekortet beställts och tillverkats skickas, enligt beskrivning i rutinen, kortkoder till den anställdas folkbokföringsadress. Det finns även en instruktion[16] som behandlar hur icke uthämtade e-tjänstekort ska makuleras.

I samband med uthämtning av kort tydliggörs ansvaret för kortinnehavare, att varje användare är personligt ansvarig för sitt kort och att detta eller kortets tillhörande koder bara får användas av kortinnehavaren. Intervjuade beskriver att det finns mycket information om hanteringen av e-tjänstekort på intranätet i syfte att tydliggöra ansvar och att befästa att e-tjänstekortet är en värdehandling.

I intervjuer med såväl chefer som funktioner inom kortorganisationen framkommer att beställning av själva e-tjänstekortet är en tydlig och väl etablerad process bland regionens medarbetare. Dock uppges den administrativa processen som startar efter att ansvarig chef lagt en kortbeställning i Självbetjäningsportalen vara omständlig och vila på manuell hantering.

I den internrevision[17] som vi nämnt tidigare i rapporten framkom vissa brister i förhållande till befintliga instruktioner kring handläggning av e-tjänstekort.

[14] Rutin 2023-03-09
[15] De kortkontor som genomför fotografering för och utlämnande av e-tjänstekort sköts av Regionservice Dalarna och finns vid regionens fyra sjukhus (Falun, Mora, Ludvika och Avesta).
[16] Uppföljning ej uthämtade kort, daterad 2019-12-09
[17] Ansvarig utgivare, biträdande ansvarig utgivare och säkerhetsansvarig.

3.2.3 Beställning och utfärdande av reservkort samt studentkort

Ett reservkort ska ha en giltighetstid på max sex månader och kortet ska vara personligt. Vidare framgår att utlämning av reservkort görs mot kvittens efter att kortinnehavaren legitimerat sig. Reservkort saknar fotografi för användaren, men ställer krav på att kortet är kopplat till HSA-katalogen, detta för att säkra spårbarhet om vem som innehar kortet.

I intervju framkommer att det krävs särskild behörighet för att utfärda reservkort. Sådan behörighet ges av kortkontoret efter deltagande i en särskild utbildning och efter godkännande från närmaste chef. Regionen uppges ha runt hundra behöriga reservkortsutfärdare, vilka vanligen har uppdrag att utfärda reservkort för den verksamhet som medarbetaren tillhör.

Reservkort uppges främst hanteras inom hälso- och sjukvården där det ofta förekommer tillfälliga anställningar och vikariat. Vi har inte tagit del av några dokument som beskriver vilken funktion som har behörighet att beställa ett reservkort. Vi får till oss att det saknas kontroll om beställning av antal reservkort samt i vilken mån ett reservkort lämnas tillbaka då den som innehaft kortet inte längre behöver det. Det uttrycks att vissa verksamheter vill ha tillgång till reservkort som kan finnas till hands om en anställd exempelvis glömt sitt ordinarie kort hemma.

I vissa fall anges de lokala kortkontoren kunna vara behjälpliga med att lösa passagebehörighet och reservkort vid akuta behov. I intervju uppges att akut utfärdade reservkort ska ha en giltighetstid på ett dygn, vilket uppges utgå från en rutin. Detta finns emellertid inte reglerat i rutinen för e-tjänstekort eller något annat dokument vi tagit del av.

Från kortorganisationen uttrycks en medvetenhet om att reservkort ibland utfärdas för att avhjälpa en akut situation trots att det strider mot gällande riktlinjer. Det framförs att dylika händelser registreras som avvikelser i regionens avvikelsehanteringssystem.

Det framhålls att hanteringen avseende reservkort har förbättringsmöjligheter. Det nämns i intervjuer att regionen behöver bli bättre på att avsluta de reservkort som inte längre behöver vara aktiva när en medarbetare på nytt använder sitt ordinarie kort efter att ha använt ett reservkort av olika anledningar.

Vi har i granskningen fått informationen att den praktiska hanteringen avseende studentkort liknar hanteringen av reservkort. Studentkorten avser medarbetare (studenter) som under begränsad tid behöver ett kort. I intervju nämns att den praktiska hanteringen innebär att ett kort handhas av studenten under hela dennes studietid, men att det ska inaktiveras då studenten inte behöver det för sin verksamhetsförlagda utbildning. Vi delges dock att det finns oklarheter med denna typ av kort, och att hanteringen avseende exempelvis avslut av korttypen studentkort kan förbättras.

3.2.4 Beställning och utfärdande av konsultkort

Korttypen är att betrakta som en ”nyckel” till lås och passage och innehas vanligen av leverantörer och entreprenörer som tillfälligt behöver ha tillgång till regionens lokaler för att kunna utföra arbete. Vi får till oss att konsultkorten saknar spårbarhet.

Vi har erhållit rutin Entreprenör, Konsultkort och Vikariekort[18]. Vi uppfattar av innehåll i dokumentet att det främst avser hantering av kort till entreprenörer. Rutinen beskriver vidare att beställning av passagekort ska göras av behörig anställd inom Region Dalarna som anger behörighet och under vilken tid kortet skall vara giltigt. Arbetsledare på externt företag ska anges tillsammans med kontaktuppgifter. Passagebehörighet kan läggas till befintligt ID06[19] kort om entreprenören har ett sådant.

Regionservice har en upprättad rutin för utlämning av nycklar/passagekort[20] som ska följas av kundtjänst och regionfastigheter. I granskningen framkommer att rutinen sannolikt inte följs fullt ut och att det härvid finns en risk att innehavare av konsultkort dels inte intygats av arbetsledare, dels inte bokförts korrekt i loggbok. I intervju framkommer vidare att detta i sin tur medför risk för att regionens kontroll över vem som innehar och hur många som innehar konsultkort är mycket låg.

Ytterligare en risk som lyfts är att medarbetare eller tillfällig personal med behov av konsultkort kopplas till HSA-katalogen i syfte att åstadkomma en enkel och effektiv hantering. Där läggs personen till i en kategori som är avsedd för hälso- och sjukvårdspersonal.

3.2.5 Bedömning

Vi bedömer att kortkontorets interna rutiner delvis säkerställer en trygg och ändamålsenlig hantering av certifikat. Vi kan i granskningen konstatera att det finns väl utarbetade rutiner, regler och system vid utfärdande av e-tjänstekort för medarbetare som erhåller en tillsvidareanställning. Vi har i granskningen emellertid konstaterat att det finns behov av att ensa rutiner, riktlinjer och intranätinformation vilket vi bedömer som en brist.

Vi bedömer att det finns både rutiner och system som säkerställer att certifikat inte läggs in felaktigt vilket regleras med fasta kontrollmoment. Endast behöriga beställare kan fatta beslut om beställning av e-tjänstekort och tillhörande behörigheter.

Vi bedömer att det inte finns tillräckliga rutiner eller system för att säkerställa att reservkort och konsultkort med certifikat läggs in och hanteras korrekt. Det finns betydande risker på grund av avsaknad av kontrollsystem för icke spårbara kort, i det fall manuell hantering och kontroll brister.

[18] Rutin 2023-10-05
[19] Standard för ID-kort som ska användas av personer som vistas på byggarbetsplatser.
[20] Rutin för utlämning av nycklar och passage, 2023-03-14

3.3 Behörighet till informationssystem

3.3.1 Krav om SITHS-kort för åtkomst till information

Behörigheter till informationssystem registreras inte på själva e-tjänstekortet utan i respektive system. Detta innebär att det ser olika ut huruvida de system som nyttjas inom Region Dalarna har infört krav om autentisering med e-tjänstekort som en andra faktor utöver användarnamn och lösenord.

Vi har i granskningen fått uppgift om att endast 50 av närmare 800 informationssystem ställer krav om SITHS-kort som andra faktor. Bland annat så har inte journalsystemet som används inom slutenvården krav om e-tjänstekortet som identifikator vid inloggning. Detta uppges bero på att verksamheten anser det alltför tidskrävande med effektivitetsförlust på grund av en mer omständlig inloggningsprocedur.

Mot bakgrund av ovan så kan vi konstatera att regionens behörighetshantering endast delvis hör ihop med hantering av e-tjänstekort. Då åtkomst och behörighet är väsentliga delar i arbetet med informationssäkerhet och det finns både regulatoriska krav och beslut i interna styrdokument om att system där känsliga uppgifter hanteras ska ställa krav om flerfaktorinloggning så redogör vi i detta avsnitt för de iakttagelser vi gjort avseende nuvarande rutiner för hantering av behörigheter oaktat hanteringen inkluderar processen för e-tjänstekort.

3.3.2 Nuvarande rutiner och process för behörighetshantering

Regionen har själva identifierat brister i nuvarande process för hantering av behörigheter och loggkontroll. Detta framgår av uppföljning dokumenterad i Informationssäkerhetsberättelse 2022, sammanställd av regionens informationssäkerhetssamordnare. Förbättringsarbete har därför initierats med syfte att utveckla processer som i högre grad är automatiserade och som dels ska bidra till att hanteringen är säkrare, dels ska avlasta cheferna. Nuvarande process uppfattas innehålla alltför stort inslag av manuell hantering. Då verksamhetschefer har ett stort ansvar för beställning, ändring och avslut av behörigheter leder den manuella hanteringen till en hög belastning på verksamhetscheferna med tanke på det stora antal användare för vilka behörigheter ska hanteras.

Regionen ska enligt uppgift under senare delen av 2023, pilottesta en mer automatiserad ”onboarding/offboarding”-process där beställning av e-tjänstekort för en nyanställd görs automatiserat som del av att ett anställningskonto upprättas i lönesystemet (HR) med koppling till HSA-katalogen. Processen ska även innefatta hantering av de grundläggande behörigheter som anställda har behov av kopplat till arbetsställe och roll. Dock uppges att tilldelning av behörigheter till verksamhetsknutna system inte kommer att ingå i det inledande utvecklingsarbetet men är något som efterfrågas på sikt.

I intervju med ansvariga från kortorganisationen framförs även från deras perspektiv att förändringsarbetet är av vikt då nuvarande modell där chefer väljer vilka behörigheter som medarbetaren ska ha, inte ger möjlighet att säkerställa en adekvat behörighetshantering.

3.3.2.1 Inför tilldelning av behörigheter

Verksamhetschefer ansvarar för att tillse utbildning och kompetens hos användare före tilldelning av behörigheter. Det ges även exempel på övergripande utbildningar om informationssäkerhet som bidragit till att öka medvetenheten om att inloggningar och e-tjänstekort är personliga.

För tilldelning av behörighet till personalkategorier och uppdrag inom hälso- och sjukvården finns dokumenterade krav på behovs- och riskanalys som ska utgöra grund för tilldelning av behörigheter. Dessa beskrivs i direktiv[21] och tillhörande rutiner[22]. Syftet uppges vara att säkerställa att behörigheten är individuell, och omfattar en tillräcklig, men inte onödigt vidlyftig mängd behörigheter. Verksamhetscheferna ansvarar för att utföra dessa riskanalyser.

Emellertid framkommer i intervjuer att det saknas kontroll över hur behörigheter faktiskt tilldelas, och om rutinbeskrivningen enligt ovan följs. Vi har under granskningen inte erhållit eller delgetts någon information huruvida dokumenterade riskanalyser ligger till grund för behörighetstilldelning. Vi noterar i granskningen att den vedertagna uppfattningen om godkännande sker vid anställning, och ej mot bakgrund av dokumenterade riskanalyser.

3.3.2.2 Tilldelning av behörigheter system

Från intervjuer uppfattar vi att behörighetstilldelning till större, centrala system fungerar men att det finns risker kopplat till verksamhetsspecifika system där inte hanteringen kan säkerställas fullt ut. Regionen har runt 600–700 datasystem där vissa förvaltas lokalt. Systemförvaltare för de lokala verksamhetssystemen ansvarar för att lägga på behörigheter till dessa utifrån lagd behörighetsbeställning. Det anses därigenom omöjligt att ha central styrning över behörighetstilldelning och den kontrollapparat som skulle behövas för att kontrollera alla behörigheter beskrivs i intervjuer vara orimlig.

I de intervjuer som genomförts med verksamhetsrepresentanter framställs behörighetshantering som komplicerad för de yrkesgrupper där standardbehörigheter inte finns. Den samlade upplevelsen är att den administrativa hanteringen anses vara så omfattande att det förekommer att fler behörigheter än vad som är nödvändigt beställs då processen ändå genomförs. I granskningen nämns även att det förekommit att behörigheter tilldelats efter önskemål, snarare än behov och att det finns en uppfattning att behörighetstilldelningen ur säkerhetsaspekt är det mest kritiska momentet i regionens hantering av e-tjänstekort.

Vi får till oss att det finns möjlighet till loggkontroller i journalsystem och att detta genomförs om det bedöms finnas behov av detta. Åtgärder vidtas enligt uppgift vid avvikelser.

Vi delges även att it-avdelningen tar fram så kallades balanslistor. Dessa beskrivs vara listor som visar avslutade anställningar och personer som inte loggat in i något system under lång tid. Till listorna följer en fråga om aktiva behörigheter ska avslutas. Genom

[21] Hälso- och sjukvården, Direktiv- behovs och riskanalys för behörighetstilldelning. Ej daterat.
[22] Rutin- Direktiv- behovs och riskanalys för behörighetstilldelning. Ej daterat.
Vårdgivarnivå- behovs och riskanalys för behörighetstilldelning. Ej daterat

intervju med verksamhetsrepresentanter konstateras att det ofta gäller studenter och annan tillfällig personal.

3.3.3 Bedömning

Vi bedömer att inte finns tillräckliga rutiner eller system för att säkerställa att behörigheter till system läggs in korrekt.

Vi konstaterar att det i styrande dokument saknas tydlighet avseende på vilka grunder som verksamhetssystem- och passagerättigheter tilldelas. Det saknas även reglering avseende hur efterlevnad av gällande regler ska kontrolleras och vem som ansvarar för detta. Vi konstaterar även här att nuvarande hantering i hög grad baseras på manuell hantering vilket medför att den mänskliga faktorn spelar en avgörande roll för att korrekta och avgränsade behörigheter tilldelas vid beställning.

Vi bedömer att dokumenterade behovs- och riskanalyser inte genomförs i enlighet med krav i Direktiv - Behovs och riskanalys för behörighetstilldelning. Vi bedömer att detta kan bero på låg kännedom om dokumenten och att de inte är fullt ut etablerade. Utifrån ovan kan vi inte utesluta att det finns risk för att hälso- och sjukvårdsnämndens verksamheter idag inte uppfyller patientdatalagens krav om att behörighet ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården.

Därtill ser vi det som allvarligt att verksamhetens effektivitet har prioriterats över följsamhet till krav i lagstiftning och interna styrdokument avseende tvåfaktorinloggning till system med känsliga uppgifter, då nuvarande journalsystem inte kräver SITHS-kort som en andra faktor vid inloggning. Detta bedömer vi som allvarligt beaktat lagstiftning, men också bristande efterlevnad till Region Dalarnas Informationssäkerhets- och dataskyddspolicy.

Vi bedömer att ansvariga i allt väsentligt har förvissat sig om att användare har genomfört obligatoriska moment (utbildning mm.) innan de tilldelas åtkomst till information.

Det finns obligatoriska utbildningar som genomförs och bedömer att den enskildes ansvar för e-tjänstekort finns väl kommunicerat till medarbetare i syfte att tillse att dessa används korrekt.

3.4 Återkallelse av e-tjänstekort och avslut av behörigheter

3.4.1 Återlämning och spärr av e-tjänstekort

Av Riktlinjer för informationssäkerhet och dataskydd för beslutsfattare framgår att ansvarig chef ansvarar för att anställdas e-tjänstekort återlämnas och spärras då anställning upphör. Därefter ska chefen destruera kortets chip och återsända det till regionens kortansvariga. Chefer kan också spärra anställdas kort vid misstanke om missbruk.

Vid förändrad anställning ska chef vid befintligt arbetsställe avsluta behörigheter, och ny chef ska beställa nya behörigheter.

Vi har bland annat tagit del av en checklista[23] som redogör för dessa moment. Av rutinen Information för chefer[24] framgår att ansvarig chef ska tillse att passagerättigheter samt verksamhetsspecifika rättigheter ska avbeställas i det fall medarbetaren byter arbetsplats inom regionen. Medarbetarens nya chef ansvarar för att uppdatera tillhörighet i såväl HSA-katalog samt specifika passagebehörigheter och systembehörigheter.

En anställd som byter arbetsplats avslutas sällan korrekt enligt intervjuade. Verksamhetsrepresentanter uppger att administration för att ta bort inaktuella behörigheter är omfattande vilket leder till att det har en tendens att bortprioriteras. Det framförs också ha fått till följd att personer som byter anställning inom regionen har kvar sitt kort och att behörigheter kopplade till den tidigare anställningen i flera fall ligger kvar.

Förklaringar som nämns är att det glöms bort eller att det finns risk att medarbetaren kommer att behöva behörigheterna framgent. Detta faktum uppges medföra att medarbetare inte sällan har för generösa behörigheter, där såväl in- och utpassering som behörigheter till verksamhetsspecifika system kvarstår. Av intervjuer upplevs detta, förutom att utgöra bristfällig efterlevnad till rutiner, också vara en betydande säkerhetsrisk.

Det finns en instruktion[25] som beskriver borttagning av certifikat och kort för personer som slutar i regionen. Enligt denna ska regionens HSA-funktion regelbundet skicka ett mejl innehållande de personer som avslutat anställningen inom Region Dalarna vilket innebär att e-tjänstekort ska avslutas. Kortet avslutas då av kortorganisationen genom avregistrering i SITHS Admin-systemet. Av rutinen framgår emellertid inte till vem HSA-funktionen ska skicka mejlet eller vem som äger rätt att avsluta kortet.

Vi får till oss att en riskbild föreligger kring återkallandet av kort och behörigheter. I intervju framförs att kortkontorets personal fyra gånger om året granskar aktiva konton i HSA-katalogen i förhållande till pågående anställningar. Det uppges att personalen återkommande upptäcker aktiva konton i katalogen trots att aktuell anställning

[23] Checklista vid avslut av anställning, ej daterad
[24] Rutin 2021-11-12
[25] Uppföljning borttagning av certifikat och kort för personer som slutat i regionen, daterad 2023-07-13

avslutats. Då detta sker skickas information till berörd chef med uppmaning om att avsluta kort och behörigheter.

Det beskrivs vara en omfattande manuell hantering att säkerställa återsändandet av e-tjänstekort samt ta bort passage- och systembehörigheter. Momenten inkluderar både chefer som ska skicka in kort och beställa ändring eller avslut av behörigheter samt HR som ska tillse avslut av anställning. Det framkommer risk att kort för tillfällig personal inte alltid återlämnas eller att tillfälliga anställningar inte avslutas i systemet.

3.4.2 Hantering av e-tjänstekort vid längre frånvaro

Vi konstaterar att det saknas rutiner för korthantering vid längre tids frånvaro.

Uppfattningen från ansvariga vid kortkontoret är att e-tjänstekort och behörigheter ska återkallas vid längre tids frånvaro och att ansvaret faller på ansvarig chef. Kortkontoret beskrivs varken ha mandat eller möjlighet att pausa kortet för långtidsfrånvarande personer.

Intervjuade verksamhetsrepresentanter uppger att det är oklart om det finns särskilda rutiner som reglerar att behörigheter och e-tjänstekort ska dras in vid längre tids frånvaro.

De intervjuade uppger att det sällan går att veta hur länge en person kommer vara frånvarande varför avaktivering av kort och behörigheter inte sker. En annan anledning uppges vara att den anställda kan behöva åtkomst till lokaler och system även vid frånvaro. De rättigheter som medarbetare har, att ta del av information och närvara vid möten med grund i arbetsmiljöregler, behöver beaktas.

Vissa system uppges känna av om ett konto varit inaktivt viss tid varpå det krävs att kontoinnehavaren ringer och beställer ett nytt inloggningslösenord då kontot ska reaktiveras.

3.4.3 Bedömning

Vi bedömer att det i allt väsentligt finns rutiner och delvis system som ska säkerställa att tilldelade certifikat återkallas när personer slutar sin anställning i regionen.

Vi konstaterar dock att rutinen inte alltid efterlevs vilket medför att ansvarig chef missar att beställa avslut och skicka in e-tjänstekort i enlighet med gällande rutinbeskrivning. I de fall detta sker bedömer vi att det finns vissa kompletterande system och rutiner som medför att e-tjänstekort med tillhörande certifikat avslutas genom kortkontorets försorg. Vi konstaterar att riskbilden är känd. Vi bedömer det som positivt att regionen har initierat ett förbättringsarbete avseende en mer automatiserad process, där beställning av e-tjänstekort och behörigheter i högre grad kommer ske med automatik vid anställning samt avslut av anställningar.

Vi bedömer att det finns rutiner som ska säkerställa att tilldelade behörigheter återkallas när personer byter arbetsställe inom regionen men vi bedömer att efterlevnad till dessa är låg.

Det medför en risk för att ett antal medarbetare i dagsläget har alltför generösa behörigheter i förhållande till sina behov för att utföra arbetsuppgifter.

Mot bakgrund av de risker vi identifierat i granskningen ser vi det som väsentligt att arbetet prioriteras och att HR-direktör och IT-direktör ges tillräckliga förutsättningar att skyndsamt få nya processer på plats. Det är viktigt, inte minst mot bakgrund av såväl patientdatalagen som regionens interna styrdokument, där vi med nuvarande hantering bedömer att det finns en avsevärd risk för att gällande regler inte efterlevs.

Vi bedömer att det saknas rutiner för hur e-tjänstekort, certifikat och tilldelade behörigheter ska hanteras vid långtidsfrånvaro eller annan längre frånvaro för anställda.

Mot bakgrund av omvärldsläget och högre risker kopplat till användares konton, lösenord och behörigheter där inaktiva konton kan utgöra högre risk för intrång eller hot, bedömer vi att frågan bör lyftas till regionens informationssäkerhetsfunktion för bedömning och ställningstagande.

3.5 Åtgärder för att upptäcka missbruk av certifikat och behörigheter

Riktlinjer för informationssäkerhet[26] reglerar att användaridentitet, e-tjänstekort och lösenord är personliga och inte får delas med andra. Enligt riktlinjen är varje användare ansvarig för sin personliga inloggning.

Huruvida riktlinjen efterlevs uppges vara svårt att kontrollera. Det framförs att sådana kontroller skulle kräva omfattande arbete, varför inga sådana kontroller genomförs i dag. De kontrollprocesser och system som i nuläget finns tillgängliga uppfattas inte kunna nyttjas för att granska detta.

I intervjuer framkommer å ena sidan en uppfattning att merparten av regionens medarbetare är mycket noggranna med sitt användande av e-tjänstekort och att utlån eller otillbörligt användande av kort är helt otänkbart. Samtidigt förmedlas att det i organisationen finns kännedom om att det har förekommit, och förekommer, att e-tjänstekort av praktiska anledningar delats mellan kollegor.

3.5.1 Bedömning

Vi bedömer att det finns väl beskrivet i styrande dokument hur e-tjänstekort och certifikat ska hanteras och förbud att dela dessa med kollegor eller andra funktioner. Vi bedömer att, utöver information, har inga ytterligare åtgärder gjorts för att minimera eller kontrollera detta.

Mot bakgrund av de regelverk och tydliga lagkrav som styr verksamheten är det väsentligt att avvikelser som medför risker för informationssäkerheten bör registreras och analyseras. Om överträdelsen inträffar inom hälso- och sjukvården äventyras därtill patientsäkerhet och sekretess.

[26] Riktlinje – Informationssäkerhet och dataskydd för användare, godkänd 2023-04-03

Datum som ovan

KPMG AB

Jenny Thörn

Kommunal revisor

Liv Ahlgren

Kommunal revisor

Veronica Hedlund Lundgren

Certifierad kommunal yrkesrevisor