Institutionen för kommunikation och information
Examensarbete i datalogi med inriktning mot nätverk- och systemadministration 15hp
B-nivå
Vårterminen 2010

Single Sign-On och Två-faktorsautentisering inom Hälso- och sjukvården

Besart Rexhepi

Single-Sign-On och Två-faktorsautentisering inom hälso- och sjukvården

Examensrapport inlämnad av Besart Rexhepi till Högskolan i Skövde, för Högskoleexamen (B.Sc.) vid Institutionen för kommunikation och information. Arbetet har handletts av Jakob Ahlin.

2010-08-20

Härmed intygas att allt material i denna rapport, vilket inte är mitt eget, har blivit tydligt identifierat och att inget material är inkluderat som tidigare använts för erhållande av annan examen.

Signerat: _____

Single Sign-On och Två-faktorsautentisering inom Hälso- och sjukvården

Besart Rexhepi

Sammanfattning

Arbetet behandlar Single Sign-On och två-faktorsautentisering inom hälso- och sjukvården. Syftet med rapporten är att undersöka eventuella utmaningar samt de möjligheter som ges vid införandet av Single Sign-On och två-faktorsautentisering i förhållande till nuvarande autentiseringsmetod. För att besvara rapportens forskningsfråga har kvalitativa forskningsintervjuer tillämpats. Även en enkätundersökning har genomförts för att få användarnas åsikter. Resultatet påvisar att en Single Sign-On-lösning tillsammans med två-faktorsautentisering uppfyller de säkerhetskrav som ställs mot hälso- och sjukvården samtidigt som det dagliga arbetet underlättas för vårdpersonalen. Men det medför även utmaningar då antalet system är många.

Nyckelord: Autentisering, Två-faktorsautentisering, Single Sign-On.

Innehållsförteckning

1 Introduktion

Att säkra nätverksresurser är en viktig del för en organisations överlevnad. För att kunna uppnå en god IT-säkerhet krävs välutformade och välplanerade säkerhetspolicies. I många fall är det företagets IT-användning och den mänskliga faktorn som skapar de största hoten inom organisationen. Tekniken däremot är endast ett hjälpmedel som används för att uppnå en god IT-säkerhet (Mitrovic, 2005).

Autentisering är en viktig del inom IT-säkerheten. Autentisering är processen som äger rum för att se till att någon/något är den/det som den utger sig för att vara. Eftersom det är betydelsefullt att skydda information men även de tjänster som hälso- och sjukvården erbjuder sina anställda, är det viktigt att på ett säkert och effektivt sätt säkra dessa resurser från obehörig åtkomst. En metod som används flitigt i dagens system är användarnamn och lösenord. Detta innebär att användarna tilldelas ett unikt användarnamn med tillhörande lösenord som användaren själv väljer eller tilldelas. Enligt Hedemalm (2001) har detta system flera fördelar. Metoden möjliggör upprättandet av ett så kallat behörighetssystem där man styr användarnas åtkomst av tjänster och information. Detta innebär att vissa användare har tillgång till vissa resurser de behöver, medan andra som inte har något med resurserna att göra inte kan nå dem. Ytterligare en fördel är att varje användare har sin egen miljö där var och en kan arbeta på vilken dator som helst i nätverket utan att uppleva någon skillnad (Hedemalm, 2001). Detta är oftast en säker metod men kan i många fall sätta höga krav på användarens minnesförmåga. Om användaren ges tillgång till endast en tjänst är det enklare för användaren att minnas lösenordet. Om användaren däremot ges tillgång till fler tjänster ökar antalet lösenord vilket kommer att ställa högre krav på användarens minnesförmåga.

Att skydda information från obehöriga är en viktig del för alla organisationer. Föreliggande studie är inriktat mot hälso- och sjukvården eftersom de hanterar känslig och sekretessbelagd patientinformation. Kärnsjukhuset i Skövde och vårdcentralen i Mariestad har studerats för att besvara studiens forskningsfråga (se avsnitt 3.1). I dagsläget tvingas vårdpersonal att använda sig av ett antal olika system, vilket gör att de måste ha ett flertal olika lösenord (Nilsson, 2008). Personalen på Kärnsjukhuset i Skövde använder sig just av detta system där varje enskild användare har ett flertal lösenord. Användarna får oftast inte välja egna lösenord utan de måste följa ett visst mönster för hur ett bra lösenord skall se ut. Detta leder till att användaren inte kan memorera lösenorden och skriver därmed ner lösenord på ”Post-It”-lappar.

I syfte att göra åtkomsten av tjänster mer användarvänlig och för att förebygga att användaren skriver ner lösenorden kan tekniken Single Sign-On (SSO) användas. Men även här kan säkerhetshot skapas och eftersom vårdpersonalen hanterar känslig och sekretessbelagd information är det viktigt med en stark autentiseringsmetod i form av en så kallad två-faktorsautentisering.

2 Bakgrund

Med grund i den tidigare forskningen kommer jag i detta avsnitt att presentera problemtiken kring autentiseringen. Avsnittet syftar till att ge en förståelse för den problematik som finns inom autentisering då användaren måste komma ihåg ett antal olika lösenord. Kapitlet kommer att beröra patientdatalagen, autentisering, autentiseringsmetoder, två-faktorsautentisering och Single Sign-On.

2.1 Patientdatalagen

Den nya patientdagalagen började gälla från 1 juli 2008. Syfter med patientdatalagen är att öka patientsäkerheten och skydda känslig information genom att bland annat reglera elektronisk tillgång till patientuppgifter.

Patientdatalagen ersätter patientjournallagen och vårdregisterlagen. Lagen ställer även högre krav på rutiner kring säkerhet och åtkomst av information. Vidare innehåller patientdatalagen bestämmelser om att en vårdgivare systematiskt ska kontrollera vårdpersonalens åtkomst av patientuppgifter (loggning) och på detta sätt förebygga obehörig åtkomst. Patientdatalagen understryker också att en vårdgivare ansvarar för tilldelningen av behörighet för åtkomst av patientuppgifter. Denna tilldelning måste begränsas till befattningshavaren och vad den vederbörande behöver för att kunna utföra det dagliga arbetet (Datainspektionen; SFS, 2008:355).

2.2 Autentisering

När en användare ska logga in mot ett system krävs det en process för att koppla användaren mot en identitet i systemet och detta kallas autentisering. Autentiseringen är ett bevis på att användaren är den person som den utger sig för att vara. Inom IT-världen kan detta ske på ett antal olika sätt, och den vanligaste autentiseringsmetoden är användning av ett användarnamn och ett lösenord. Eftersom människor har svårt att komma ihåg lösenord samt att lösenorden inte alltid bevaras konfidentiellt är den här metoden inte lämplig i alla situationer. I den ”riktiga” världen kan vi människor identifiera oss på ett antal olika sätt. Några sätt att identifiera sig på är med hjälp av ett pass, körkort, ID-kort eller med våra unika personliga och fysiska egenskaper som till exempel ansikte och röst. I datorvärlden kan säker identifiering ske på ett antal olika sätt (se avsnitt 2.3).

2.3 Autentiseringsmetoder

För att en enskild användare ska kunna autentisera sig mot ett system och för att bevisa att en användare är den som den utger sig för att vara finns det ett antal olika metoder. Enligt Sitic (2008) kan användaren autentisera sig med hjälp av bland annat:

- Något användaren ***kan***: *lösenord.*
- Något användaren ***har***: *smarta kort, säkerhetsdosa, certifikat osv.*
- Något användaren ***är***: *fingeravtryck, skanning av iris.*

2.3.1 Lösenord

I dagsläget är användarnamn och lösenord den vanligaste autentiseringsmetoden för att skydda information eller resurser från obehöriga. Enligt Mitrovic (2005) är lösenord den första nivån av säkerhet och därför bör den aldrig förbises. Beroende på

kombinationen av bokstäver, nummer och symboler varierar lösenords säkerhetsgrad. Lösenordens komplexitet och möjliga kombinationer illustreras i Tabell 1.

Tabell 1: Kombination av tecken och längd i lösenord kan ge många kombinationer (Mitrovic, 2005, s.151).

	Lösenod	**Möjliga kombinationer**
Bokstäver (2)	Ab	676
Bokstäver (4)	Abcd	456 976
Bokstäver (7)	Abcdefg	8 miljarder
Bokstäver och siffror (7)	A1b2c3d	78 miljarder
Bokstäver, siffror och symboler (6)	A1@b2%	98 miljarder
Bokstäver, siffror och symboler (7)	A1@b2%c	6700 miljarder

2.3.1.1 Problem med lösenord

Eftersom människan är den svagaste länken för att uppnå god IT-säkerhet är användandet av lösenord inte alltid det bästa alternativet för att skydda känslig information. För att uppnå god IT-säkerhet är tumregeln att människan ska stå för 80 % av säkerheten (Mitrovic, 2005) vilket medför ett stort ansvar för användaren. Eftersom organisationer växer sig allt större ökar även antalet IT-system, vilket innebär att användarna i många fall måste komma ihåg ett antal olika lösenord för att kunna utföra det dagliga arbetet. Med tanke på detta ökar även säkerhetsriskerna då användare skriver ner, återanvänder eller använder för enkla lösenord som till exempel namn eller personnummer (Westerlund, 2008).

Enligt Mitrovic (2005) ska ett bra lösenord vara minst sju tecken långt och innehålla bokstäver, nummer och symboler. Ett exempel på ett bra lösenord är enligt Mitrovic (2003):

- R23<Bol

Det är dock inte tillräckligt att endast ha ett komplext lösenord, utan det måste även bytas ut med jämna mellanrum. Mitrovic (2003) hävdar att *”lösenordet är som en tandborste, använd det varje dag, dela inte det med någon och byt det vid vissa intervaller”* (Mitrovic, 2003, s. 137). Kravet på att ett lösenord skall bytas med jämna mellanrum och utformas efter ett särskilt mönster innebär ytterligare krav på användarens minnesförmåga. Användarna tvingas komma ihåg komplexa lösenord som inte har någon personlig innebörd. Det nya lösenordet måste också skilja sig rejält från de sex senast använda lösenorden (Mitrovic, 2003). Krav på hur ett lösenord skall se ut kan leda till att användarna för ner lösenorden på papper eller mobiltelefoner vilket ökar risken för obehörig åtkomst. Om verksamheten däremot inte har krav på hur ett lösenord skall se ut är det vanligt att användarna återanvänder eller använder enkla lösenord som till exempel namn, personnummer osv. Även här uppstår en säkerhetsrisk genom att obehöriga kan chansa sig till lösenordet.

> *”Att skydda sitt lösenord handlar om att inte skriva ner det, aldrig visa den för någon och inte tillåta att någon tittar över axeln när du skriver in det” (Mitrovic, 2003, s. 137)*

Idag finns även många program ute på Internet för att knäcka lösenord och därför är inte lösenordsautentiseringen den bästa metoden för att uppnå god IT-säkerhet. Med tanke på att användare har en tendens att välja enkla lösenord kan en så kallad ”ordlista-attack” användas för att knäcka lösenord. Attacken innebär att ett program använder sig av en ordlista för att sedan väldigt snabbt undersöka ordlistan som innehåller namn, uttryck, siffror och kombinationer av dessa för att förhoppningsvis knäcka lösenordet. Enligt (Carling, 2007) är lösenord inget som kommer att försvinna helt utan kommer att användas och leva kvar tack vare sin enkelhet.

2.3.2 Smarta kort

Smarta kort är en autentiseringsmetod som är grundad på något som användare *har*. Tekniken är tillräckligt mogen för att företag och organisationer ska våga använda sig av den. Smarta kort ser ut som vanliga kreditkort men dessa kort har en inbyggd mikroprocessor och ett minne (Stamp, 2006). Eftersom kortet har en mikroprocessor kan det göra enklare uträkningar. För att öka säkerheten kombineras smarta kort ofta med en PIN-kod vilket innebär att man använder sig av två-faktorsautentisering, det vill säga lösenord tillsammans med något som användare har. Enligt Carling (2007) använder många företag redan smarta kort då dessa används för att komma in i byggnader och rum, men dessa kort används även till inloggningar mot företagets datorer. Säkerhetsexperter tvivlar inte på att smarta kort är betydligt säkrare än traditionella metoder för autentisering (Carling, 2007). Användningen av smarta kort utgör en utmärkt metod för att hantera SSO. Eftersom det i många fall förekommer att användare måste komma ihåg ett antal olika lösenord och göra ett antal olika inloggningar för att komma åt de system som den behöver är SSO en eftertraktad teknik (se avsnitt 2.5). För att lösningen med smarta kort ska vara möjlig krävs det att varje dator är utrustad med en kortläsare. En del bärbara datorer har inbyggda kortläsare, men majoriteten av datorerna som finns ute på marknaden saknar kortläsare. Därför måste man använda externa läsare som måste anpassas och vara kompatibla med operativsystemen som används i företaget (Carling, 2007).

2.3.3 Biometri

Biometrisk autentisering är grundad på något användaren *är*. Det finns ett antal olika metoder för att autentisera sig när biometrisk autentisering används. Metoderna som kan användas är till exempel skanning av ett fingeravtryck eller iris.

Biometri är den äldsta metoden för igenkänning. Människan känner igen varandra genom ansiktet eller genom rösten då man till exempel pratar i telefon. En stor fördel med biometrisk autentisering är att det är svårt att förfalska eller stjäla en användares yttre fysiska egenskaper (Schneier, 1998). Genom biometri används användarens unika kroppsdelar för att identifiera denne mot något. En biometrisk autentisering fungerar genom att till exempel användaren lägger sitt finger på en scanner som sedan jämför det scannade fingeravtrycket med dennes fingeravtryck som finns lagrat i en databas. Biometri är självklart inte ett helt säkert system då det går att stjäla en enskild användares fingeravtryck. I vissa fall kan systemet även luras och särskilt då man har ett bra kort på en användares öga/iris. Enlig Stamp (2006) är dessa attacker fullt möjliga men självklart går det att förhindra dessa genom att scanningsapparaten riktar

ett ljus mot ögat för att säkerhetsställa att ögat är riktigt och inte ett foto innan jämförelsen mot databasen genomförs.

Det största problemet med biometrisk autentisering är att systemet kan autentisera användare B som användare A. Omfattningen av dessa kallas även för ”fraud rate” (Stamp, 2006). Det finns även andra fel då till exempel användare A försöker autentisera sig mot ett system som den har rättigheter till men trots detta nekas åtkomst. Omfattningen av dessa kallas för ”insult rate”. För att höja säkerheten hos biometriska system kan *fraud rate* höjas men detta leder istället till att *insult rate* blir väldigt hög, det vill säga att en användare nekas åtkomst trots att denne har rätt till åtkomst (Stamp 2006). Sänker man emellertid *fraud rate* minskar även *insult rate* och användare som har rätt till åtkomst kommer inte att nekas det, men samtidigt höjs riskerna för att obehöriga ska få tillgång till system de inte har rättigheter till. Enligt Stamp (2006) fungerar biometriska system bäst då *fraud rate* och *insult rate* ligger på lika höga säkerhetsnivåer.

Det finns många fördelar med biometrisk autentisering men det finns även nackdelar, till exempel om man ställs inför situationen att en biometrisk ”nyckel” hamnar i orätta händer. Ett lösenord går alltid att byta men biometriska ”nycklar” är alltid unika och går inte att förändra (Stamp, 2006). Enligt Stamp (2006) kommer användningen av biometrisk autentisering att öka i framtiden då det förhoppningsvis blir billigare och mer beprövat.

2.4 Två-faktorsautentisering

Vid användning av lösenord kan man aldrig vara säker på att det är rätt person som har fått tillgång till de tjänster och resurser som varit lösenordsskyddade. Utan systemet *förutsätter* att det är rätt person som har fått tillgång tjänsterna och resurserna eftersom denne har angivit rätt lösenord. Med tanke på detta är det ytterst viktigt med en stark autentisering, det vill säga väldigt starka lösenord (som inte är det bästa alternativet med tanke på att människor har svårt att kom ihåg lösenord och speciellt när det är ett antal olika lösenord) eller en två-faktorsautentisering. Enligt Sitic (2008) innebär två-faktorsautentisering att användaren autentiserar sig med två av följande saker:

- Något användaren ***kan***: *lösenord.*
- Något användaren ***har***: *smarta kort, säkerhetsdosa, certifikat osv.*
- Något användaren ***är***: *fingeravtryck, skanning av iris.*

Exempel på två-faktorsautentisering:

1. *Lösenord + Engångslösenord eller smarta kort*
2. *Lösenord + Fingeravtryck*

Det finns även tre-faktorsautentisering men den metoden bör inte användas inom hälso- och sjukvården då det tar för lång tid att autentisera sig. Tre-faktors autentisering innebär att användaren autentiserar sig med hjälp av tre saker: något användaren kan, har och är. Ett exempel är: *lösenord, smarta kort och fingeravtryck.*

Fördelen med två-faktorsmetod är att man får en stark och säker autentisering för att skydda känslig information. Att skydda information från obehöriga är viktigt för de flesta företagen idag och inte bara inom hälso- och sjukvården. För att lösa problemet

med ”Post-It”-lappar och för att höja användarvänligheten för en användare är metoden utmärkt att genomföra tillsammans med SSO. Fördelen med SSO är att användaren då endast behöver komma ihåg ett lösenord till alla tjänster och resurser som denne har tillgångsrättigheter till. SSO stöder även två- och tre-faktors autentisering då en stark autentiseringsmetod är att föredra (Loshin, 2001).

2.5 Single Sign-On

Single Sign-On (SSO) är en teknik som kan bidra till att lösa problemet med lösenordshantering och höja användarvänligheten för en slutanvändare. Metoden förespråkas av många verksamheter och forskare.

SSO kan tolkas olika från person till person men definitionen som används i denna rapport är att användaren autentiserar sig en gång mot en autentiseringsserver med ett användarnamn och ett lösenord eller annan metod för att sedan få tillgång till alla tjänster som denne har behörighetsrättigheter till. Användaren ska inte behöva autentisera sig på nytt varje gång en ny tjänst ska användas, utan detta ska ske automatiskt.

Genom att använda sig av SSO-tekniken kan en användare komma åt alla tjänster som denne har behörighetsrättigheter till genom att autentisera sig en gång. Tekniken ska underlätta det dagliga arbetet för användarna men även förebygga säkerhetsrisken som uppstår då slutanvändare har olika lösenord till olika tjänster. Genom att endast behöva komma ihåg ett lösenord minskar riskerna för att användaren skriva ner, återanvänder eller använder för enkla lösenord. Detta leder till att användaren inte behöver lägga ner lika mycket tid på att logga in i de olika systemen som behövs för att utföra sitt arbete. Vid användning av SSO-tekniken minskas även supportkostnaderna dramatiskt eftersom användare endast har ett lösenord att memorera (Loshin, 2001).

En stor nackdel med SSO är att det är ”fritt fram” för en inkräktare om det första lösenordet knäcks. SSO-tekniken bör därför kombineras med en starkare autentisering än lösenord som till exempel smarta kort eller biometriska läsare (Carling, 2007).

2.6 BIF – Bastjänster för Informationsförsörjning

Inom hälso- och sjukvården är det som grundkrav att patientinformation hanteras på ett säkert sätt, att rätt personal ska ha tillgång till rätt information och att ingen obehörig ska få komma åt informationen. För att säkerställa att information hanteras på ett korrekt sätt inom men även mellan organisationer är det ytterst viktigt med en gemensam infrastruktur för IT-säkerhet. Bastjänster för informationsförsörjning (BIF) är en grundpelare i den gemensamma infrastrukturen (Fredriksson, 2008). BIF består av nio olika bastjänster och dessa tjänster har till syfte ett erbjuda en säker hantering av information mellan IT-system inom hälso- och sjukvården. De nio bastjänsterna är:

- Autentisering
- Åtkomstkontroll
- Samtycke
- Vårdrelation
- Utlämnande

- Säker patientkontext
- Notifiering
- Loggning
- Logganalys

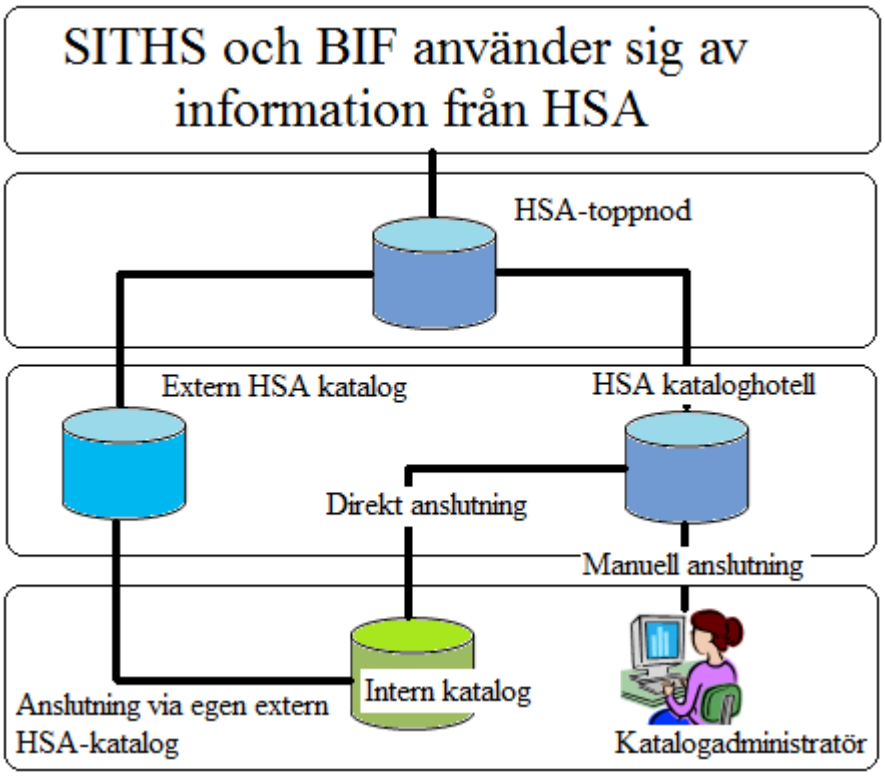
BIF kan hantera patientdatalagens krav på bland annat stark autentisering, åtkomstkontrell, logg och logganalys.

2.7 SITHS – Säker IT inom Hälso- och Sjukvården

Säker IT inom Hälso- och Sjukvården (SITHS) är en del av den tekniska infrastrukturen som ingår i nationell IT-strategi för hälso- och sjukvården. För att vårdpersonalen ska kunna identifiera sig på ett säkert sätt används en säkerhetslösning där varje anställd har ett personligt elektroniskt ID-kort med elektroniska legitimationer som i sin tur möjliggör säker identifiering och kryptering av känslig information (Näsberg, 2010). SITHS-korten möjliggör ett antal olika funktioner som till exempel SSO, inloggning mot IT-system och elektroniskt signerade journalhandlingar, recept, avtal och fakturor (Näsberg, 2010). För att få ansluta sig till SITHS ställs det krav på landsting, kommuner eller privata vårdgivare. Några krav är att de måste vara anslutna till Sjunet och HSA (Näsberg, 2010).

2.8 HSA – Hälso- och Sjukvårdens Adressregister

Hälso- och Sjukvårdens Adressregister (HSA) är en så kallad toppnod för att sammanbinda lokala kataloger (Gravin, 2008). HSA-katalogen ska innehålla information om personer, enheter och funktioner där informationen är en delmängd av en organisations interna katalog. HSA består av flera delar som bland annat ett gemensamt kataloghotell och en extern HSA-katalog. HSA-toppnoden ska därefter knyta samman dessa kataloger. Bilden nedan visar kopplingen till HSA (Johansson, Sjukvårdsrådgivningen, 2009).



Figur 1: Teknisk infrastruktur för HSA (efter Johansson, 2009, s. 8).

Det finns ett antal olika sätt att ansluta sig till HSA-katalogen. Ett alternativ är att synkronisera de interna katalogerna mot HSA-kataloghotell. Detta innebär att information som finns på de interna katalogerna synkroniseras med HSA-kataloghotell. Med synkronisering menas att om information läggs till, ändras eller tas bort från en plats, så speglas exakt samma process på andra sidan. Andra metoden är att använda sig av ett webb-baserat administrationsgränssnitt. För att detta ska vara möjligt krävs ett admingränssnitt, IP-adress samt ett användarnamn och ett lösenord vilket delas ut av Carelink (se avsnitt 4.2). Tredje och sista metoden för att ansluta sig mot HSA-katalogen är genom att använda sig av protokollet DSP. Den interna katalogen ansluts mot den egna externa katalogen som är uppbyggd enligt ett HSA-schema. Användandet av DSP-protokollet, som används för att spegla information från den interna till den egna externa HSA-katalogen, medför mer ansvar för organisationen. Detta innebär att sjukhuset måste ansvara för drift och säkerhet i den egna externa HSA-katalogen (Johansson, Sjukvårdsrådgivningen). Informationen som sparas i HSA-katalogen används av bland annat SITHS och BIF och därför är det en av de viktigaste grundpelarna tillsammans med Sjunet (Inera, 2010).

2.9 SSO och två-faktorsautentisering i landsting och kommuner

I det följande presenteras en beskrivning av ett antal landsting och kommuners status gällande tillämningen av SSO och två-faktorsautentisering (för urvalsbeskrivning se avsnitt 4.2).

2.9.1 Karlstad kommun

Karlstads kommun fick Sveapriset 2009 för ”Smart arbetsplats”. Eftersom det är krav på stark autentisering inom hälso- och sjukvården används SITHS-korten som är en del av Nationella IT-strategin för hälso- och sjukvården. SITHS-korten ska inte bara

uppfylla de krav som ställs på stark autentisering utan det ska även förenkla vårdpersonalens arbete då en SSO-lösning möjliggörs. En sjuksköterska som uttalat sig i rapporten hävdar att all krångel med lösenord minskar och man enklare kan avbryta arbetet för att fortsätta med det på en annan avdelning (Inera, 2010). Varje dator har ersatts av smarta arbetsplatser (tunna klienter) och dessa arbetsplatser sköter endast tre funktioner, kort för inloggning, samordnad inloggning och tillträde till sin egen dator från olika ställen (Inera, 2010). Enligt G. Kartman (personlig kommunikation, 12 maj, 2010) är Smart arbetsplats uppbyggt kring terminalserverfunktionalitet både när det gäller lastbalansering, sessionåterupptagning och kryptering mellan serversidan och den tunna klienten.

2.9.2 Örebro läns landsting

I Örebro läns landsting har man enligt J. Bjärvall (personlig kommunikation, 14 juni, 2010) delat upp SITHS-projektet i två delar där den första handlade om att bygga infrastruktur, det vill säga organisationen, utformning av korten, rutiner och med mera. Till en början användes korten på länets tre sjukhus som passerkort. Enligt Respondent D handlar nästa steg om att bredda användningen av korten. Nu är det fler och fler av deras IT-system som stödjer SITHS-korten som idag används för autentisering. Enligt J. Bjärvall (personlig kommunikation, 14 juni, 2010) har de även en SSO-lösning där de använder sig av en portallösning, Klinisk Portal, som nu också stödjer SITHS-kortet. De har dock ingen bra lösning vad gäller sessionshantering, utan genomför tester för att hitta en lösning som klarar av mängden användare och IT-system.

2.9.3 Landstinget i Östergötland

I Landstinget i Östergötland ska en journalportal breddinföras under 2010. Journalportalen ska vara en samlingsportal för vårdapplikationer som i sin tur förenklar arbetet för användaren då de kan ansluta till vårdapplikationerna genom endast en inloggning (Medin, 2010).

3 Problemformulering

Allt eftersom en organisation växer ökar även antalet IT-system inom organisationen. Fler IT-system betyder att användaren i många fall måste komma ihåg ett antal olika lösenord. Detta innebär att ett antal inloggningar måste genomföras för att användaren ska kunna komma åt de resurser som krävs för att utföra sitt arbete. I och med detta försämras inte bara användbarheten utan säkerhetsproblem kan även uppstå eftersom det förekommer att användaren skriver ner eller återanvänder gamla lösenord.

Inom hälso- och sjukvården hanteras känslig information som är sekretessbelagd och därför är det viktigt att informationen inte hamnar i orätta händer. Så som situationen ser ut idag tvingas vårdpersonalen logga in och ut från ett flertal olika system. Detta leder till att vårdpersonalen måste komma ihåg ett antal lösenord för att komma åt den information de behöver för att utföra sitt arbete. I många fall leder detta till säkerhetshot då personalen skriver ner lösenorden på papper och förvarar dem nära datorn (Nilsson, 2008).

Inom vården, så som för många andra organisationer, är det viktigt med förenklade inloggningsrutiner. Men även behörighetssystem är viktigt för att förhindra obehöriga från information och resurser. Enligt Ricknäs (2004) har det skett ett flertal gånger genom åren att obehörig personal tittat på journaler som de inte har rättigheter till när kändisar lagts in på sjukhus. Det förekommer även att personalen läser bekantas journaler. Enligt Östnäs (2010) har en sjuksköterska dömts till dagsböter efter att ha tjuvläst bekantas journaler. För att undvika att information hamnar i fel händer är det ytterst viktigt att användarna kan identifiera sig inom hälso- och sjukvården. Med tanke på säkerhetshoten som skapas då användarna måste komma ihåg ett antal olika lösenord till ett antal olika tjänster krävs ett nytt system för personidentifiering. En teknik som skulle förenkla inloggningsrutinerna men även öka effektiviteten i arbetet är SSO.

SSO-tekniken förenklar inloggning till de tjänster som personalen har tillgångsrättigheter till, men det kan dock uppstå säkerhetshot med tanke på att lösenord fortfarande används. Eftersom hälso- och sjukvården hanterar känslig och sekretessbelagd information är det viktigt att använda en användarvänlig men också stark autentiseringsteknik. Stark autentisering innebär att användaren autentiserar sig på två sätt, med ett lösenord som användaren kan utantill men också med ett så kallade smarta kort, fingeravtrycksläsare eller en säkerhetsdosa som genererar ett engångslösenord.

Efter en analys av tidigare forskning verkar det som att det fortfarande inte finns någon forskning utförd om möjligheter och utmaningar vid införandet av SSO och två-faktorsautentisering inom hälso- och sjukvården vilket motiverar denna studie.

3.1 Syfte och problemspecificering

Med utgångspunkt i problemformuleringen har detta projekt till syfte att undersöka eventuella utmaningar samt de möjligheter som ges vid införandet av SSO samt två-faktorsautentisering i förhållande till nuvarande autentiseringsmetod. Med tanke på de säkerhetsbrister som uppstår vid användandet av lösenord som autentiseringsmetod är det viktigt med stark autentisering såsom smarta kort, fingeravtryck eller säkerhetsdosa. Med utgångspunkt i detta är rapportens övergripande forskningsfråga:

- *Vilka eventuella utmaningar samt möjligheter ges vid införandet av SSO och Två-faktorsautentisering i förhållande till nuvarande autentiseringsmetod?*

3.2 Avgränsning

Undersökningen har begränsats genom att studera hur situationen ser ut på Kärnsjukhuset i Skövde: vilken typ av autentisering som används i dagsläget, vilka eventuella utmaningar Kärnsjukhuset i Skövde ställs inför vid införandet av SSO och två-faktorsautentisering, samt de möjligheter som föreligger vid införandet av SSO och två-faktorsautentisering. En enkätundersökning har även genomförts för att få vårdpersonalens åsikter om de befintliga systemen och deras inställning till SSO och två-faktorsautentisering. Enkätundersökningen utfördes på vårdcentralen i Mariestad.

4 Metod

Detta kapitel har till syfte att ge en beskrivning av de metoder som används för att besvara projektets forskningsfråga.

4.1 Metodval

Syftet med framförliggande uppsats är att undersöka eventuella utmaningar samt de möjligheter som ges vid införandet av SSO samt två-faktorsautentisering inom hälso- och sjukvården. Eftersom analysen av den tidigare forskningen visar att det finns en viss forskning om utmaningar och möjligheter vid införandet av SSO och två-faktorsautentisering inom hälso- och sjukvården, bedömer jag att en kvalitativ ansats är lämplig att använda för att kunna besvara studiens forskningsfråga.

Om man vill undersöka hur människor upplever olika företeelser ska ett kvalitativt perspektiv anammas (Bell, 1995). Genom anammandet av kvalitativa metoder får man därmed insikt i hur människor upplever och beskriver olika företeelser. Enligt Starrin och Svensson (1994) handlar metoden om att ”förstå mänskliga handlingar, erfarenheter och beteenden”, men även att komma åt ”motiv, avsikter, innebörder och föreställningar”. Enligt Denscombe (2000) associeras kvalitativa metoder med ”täta beskrivningar”, det vill säga detaljerade och ingående beskrivningar. Därför tenderar den kvalitativa metoden att innefatta få människor samt ha ett avgränsat omfång.

Kvalitativ data kan nås genom olika metoder. För att producera djupgående data och för att besvara projektets forskningsfråga anser jag att kvalitativa forskningsintervjuer är bäst lämpade för projektet. Det finns olika varianter av forskningsintervjuer: *strukturerad*, *semistrukturerad* och *ostrukturerade* intervjuer. Den strukturerade intervjuformen innebär att forskaren i förväg har konstruerat ett antal frågor med svarsalternativ som respondenten ska ta ställning till. Vid semistrukturerade intervjuer däremot har forskaren på förhand konstruerade frågor som respondenten ska svara på. Svaren är alltså öppna och respondenten ges möjlighet att tala mer uttömmande om ämnet. Med den ostrukturerade intervjuformen ges respondenten möjlighet att fritt tala om ämnet och forskaren ska ingripa så lite som möjligt under intervjun (Dahlberg, 1997). Eftersom jag vill ha djupgående svar har jag valt att göra semistrukturerade intervjuer där frågorna styr respondenten i viss mån, men samtidigt får denne möjlighet att uttrycka sina tankar och idéer kring ämnet.

Eftersom vårdpersonalens åsikter om de befintliga systemen och deras inställning till SSO-lösning är en viktig del för att besvara studiens forskningsfråga, anser jag att även en enkätundersökning är nödvändig. Enligt Bell (1995) är en enkätundersökning en bra metod att använda då man ska samla in en viss typ av information på ett enkelt och effektivt sätt. För att få användarens åsikter och tankar ska enkäterna vara semistrukturerade vilket innebär att varje fråga ska ha ett antal olika svarsalternativ, men även att användaren ska ges möjlighet att svara på frågan med egna ord. Genom att ge användarna denna möjlighet kan man få en djupare förståelse för deras svar, samtidigt som man får både en kvalitativ och en kvantitativ mätbar data. En fördel med enkätundersökningen är att man har möjlighet att rikta in sig på en större grupp människor samt att den inte är lika tidskrävande som intervjuerna att genomföra. En annan fördel är att respondenterna har möjlighet att besvara enkäten när de har tid. Nackdelen är dock att frågorna kan tolkas olika och missförstås. En annan nackdel är att de öppna frågorna där respondenten själv kan skriva sina åsikter oftast lämnas

blanka. För att uppnå bästa resultat ska man enligt Bell (1995) göra ett så kallad pilottest innan man skickar ut sina enkäter till respondenterna, just för att säkerställa frågornas relevans och minimera risken för feltolkningar.

4.2 Urval av respondenter och avgränsning

Urvalet av respondenter har varit mycket begränsat eftersom arbetet samt forskningsfrågan endast är inriktad på Kärnsjukhuset i Skövde. Eftersom det finns ett begränsat personalantal som besitter den eftersökta kompetensen har det omöjliggjort ett brett urval av respondenter. Syftet med framförliggande arbete är inte att generalisera, utan snarare att undersöka eventuella utmaningar Kärnsjukhuset i Skövde ställs inför samt de möjligheter som ges vid införandet av SSO samt två-faktorsautentisering. Utifrån detta anser jag inte att antalet respondenter är för få för att uppnå arbetets syfte.

Efter rundringning och kontakt via e-mail med personal från Kärnsjukhuset i Skövde var det *en* respondent som ville medverka i undersökningen. Eftersom intresset från Kärnsjukhusets personal var ytterst svalt togs även kontakt med personal från Carelink, som är en del av Sjukvårdsrådgivningen SVR AB. Visionen som Carelink har är att samla alla aktörer inom vård och omsorg i en organisation för att på så sätt skapa en gemensam syn på hur IT kan och bör användas inom vården.

Utöver intervjuerna har enkäter delats ut på vårdcentralen i Mariestad. Enkäterna var avsedda att delas ut på Kärnsjukhuset i Skövde, men av olika skäl fick jag inte göra detta och därmed blev jag tvungen att välja ett nytt sjukhus för att över huvud taget kunna slutföra undersökningen. Syftet med enkäterna är att undersöka hur användarna ser på det befintliga autentiseringsmetoden. Men de syftar också till att undersöka hur användarna ställer sig till en SSO-lösning där autentiseringen sker med hjälp av ett personligt kort istället för lösenord.

För att undersöka vad andra landsting och kommuner har för status vad gäller SSO och två-faktorsautentisering valde jag att ta kontakt via e-mail. Det skedde ett slumpmässigt urval av landsting och kommuner. Följande fick ett e-mail (se Bilaga C): Landstinget i Östergötland, Landstinget i Uppsala län, Landstinget i Jönköpings län, Region Skåne, Landstinget i Kalmar län, Landstinget Kronoberg, Landstinget Blekinge, Örebro läns landsting och Karlstads kommun. Av dessa var det Karlstads kommun, Örebro läns landsting och Landstinget i Östergötland som svarade.

4.3 Datainsamling

Den data som ligger till grund för framförliggande arbete har samlats in med hjälp av två olika metoder, primär respektive sekundär datainsamling. Den primära datainsamlingen har skett genom kvalitativa semistrukturerade intervjuer och semistrukturerade enkäter. Den sekundära datainsamlingen har däremot skett genom inläsning av litteratur, artiklar och annat relevant material. Fördelen med den sekundära datainsamlingsmetoden är att den inte är lika tidskrävande som intervjuer och enkäter. En annan fördel är att insamlingen och inläsningen av data kan ske under arbetes gång. En nackdel är dock att det kan bli svårt att sortera den information man hittat och det finns en risk för att informationen är inaktuell samt opålitlig.

4.4 Planering och genomförande av intervjuer och enkäter

När det gäller planering och genomförande har det första delmålet varit att konstruera intervjufrågor för att därefter genomföra ett pilottest. De semistrukturerade intervjufrågorna har konstruerats med utgångspunkt i arbetets forskningsfråga. Vidare har jag genomfört ett pilottest där jag har intervjuat en person. Genom pilottestet har jag kunnat säkerställa frågornas relevans och formuleringar. Eftersom jag inte har någon tidigare erfarenhet av intervjuer har pilottestet varit till stor nytta och en viktig personlig läroprocess. Under tiden som frågorna konstruerades tog jag kontakt med respondenterna via telefon. Enligt Bell (1995) är det viktigt att låta respondenterna komma med egna önskemål när det gäller tid och plats för intervjuernas genomförande, och därför har respondenterna själva fått bestämma plats och tid för intervjuns genomförande. I enlighet med de forskningsetiska rutinerna som finns har respondenterna vid första kontakten, men även vid intervjutillfället, blivit informerade om projektets syfte, i vilket sammanhang det genomförs, att deras medverkan är frivillig samt att materialet och deras personuppgifter kommer att behandlas konfidentiellt.

Intervjuerna har spelats in genom användandet av en diktafon. Enligt Dahlberg (1997) ska forskningsintervjuerna spelas in för att underlätta analysarbetet. Intervjun med respondent A (se avsnitt 4.5.1) skedde på Kärnsjukhuset i Skövde på respondentens kontor. Eftersom vi satt avskilt förhindrades avbrott och moment som kunde ha stört intervjun. Intervjun med respondent A varade i cirka 30 minuter. Intervjun med respondent B (se avsnitt 4.5.1) skedde via telefon, och även den spelades in med hjälp av diktafon. Vid intervjuns genomförande satt respondenten i en bil, men trots detta genomfördes intervjun utan störningsmoment. Intervjun med Respondent B varade i cirka 10 minuter. Intervjufrågorna skickades till respondenterna i god tid innan intervjutillfällena just för att ge dem möjlighet att fundera kring frågorna. Samma frågor har ställts till de medverkande men även följdfrågor har förekommit.

Jag har ovan (se avsnitt 4.1) berört relevansen av användarnas åsikter om de befintliga systemen och med grund i detta utformade jag en semistrukturerad enkät. Innan enkäten lämnades till sjukhusets personal genomfördes ett pilottest eftersom det är ytterst viktigt att frågorna tolkas likadant. Enligt Bell (1995) skiljer sig ordens innebörd från person till person och därför är det viktigt att tänka på hur en formulering kan tolkas av olika respondenter. Istället för att göra enkätutskicket via posten lämnade jag personligen enkäterna till en informationsansvarig på vårdcentralen i Mariestad och denne delade ut enkäterna till respondenterna. Enligt Bell (1995) är det en fördel att personligen dela ut enkäterna eftersom man kan förklara undersökningens syfte och i vissa fall kan man få enkäterna ifyllda på en gång.

Jag delade ut 20 enkäter och 15 respondenter besvarade enkäterna. Utifrån detta kan man konstatera att bortfallet är fem enkäter. Bell (1995) menar att ett stort bortfall kan ge skeva resultat och därför bör man anstränga sig för att göra bortfallet så litet som möjligt. Jag anser att ett bortfall på fem enkäter är acceptabelt och jag anser inte att bortfallet kommer att påverka resultatet nämnvärt.

4.5 Bearbetning och analys

Efter varje intervjutillfälle har intervjuerna transkriberats och skrivits ut. Transkriberingen är ett tidskrävande arbete, men jag anser att transkriberingen är en

viktig del av processen eftersom bearbetningen av materialet underlättar analysen. Enkäterna har sammanställts genom att jag har gått igenom enkätsvaren fråga för fråga. Svaren från varje enskild fråga samt respondenternas egna åsikter har sedan förts in ett sammanställningsdokument som utformades utifrån enkätformuläret (jämför Bilaga A med B).

4.5.1 Presentation av respondenterna

Jag har valt att inte uppge respondenternas identitet och därför har jag valt att koda dem genom att kalla de för ”Respondent A” och ”Respondent B”. Det enda som kommer att framgå är respondenternas kön, utbildning, tidigare erfarenheter samt nuvarande sysselsättning. Följande kan sägas om respektive respondent:

Respondent A: Har en civilingenjörsutbildning inom datateknik. Han har arbetat som konsult inom olika företag, bland annat för Sony Ericsson. Under de två senaste åren har Respondent A arbetat som IT-strateg på sjukhuset i Skövde där han arbetar med olika datafrågor samt ägnar en stor del av sin arbetstid till administration.

Respondent B: Har en universitetsutbildning med matematik, fysik, elektronik och datateknik i botten. Respondent B är förvaltningsansvarig för HSA där hans ansvar är att HSA vidmakthålls och vidareutvecklas efter omgivningens krav och behov. Har ekonomisk och funktionellt ansvar för HSA.

5 Resultat och analys

I det här avsnittet presenteras resultatet av intervjuerna och enkätundersökningen.

I dagsläget använder sig Kärnsjukhuset i Skövde (KSS) av lösenord som autentiseringsmetod och en SSO-lösning bedöms svår att implementera då hundratals olika system används. KSS använder en så kallad gruppinloggning där ett antal olika användare har ett gemensamt användarnamn och lösenord till klientdatorn, men personliga användarnamn och lösenord används då de till exempel ska läsa eller skriva i journalsystem. Eftersom KSS inte har en SSO-lösning måste användarna komma ihåg ett antal olika lösenord och detta kan leda till problem. I resultatet kommer inte alla frågor som ställdes i enkäten att beröras, men de sammanställda resultaten av enkätundersökningen går att finna i Bilaga B.

5.1 Nuvarande autentiseringsmetod

Eftersom det inte finns datorer till varje användare uppstår det problem om en anställd loggar in och dennes inloggning används därefter resten av dagen. För att lösa detta problem använder sig KSS av gruppinloggningar då ett antal olika användare har ett gemensamt användarnamn och lösenord för att logga in på klientdatorn/arbetsstationen. När användaren ska jobba mot andra system som till exempel journalsystem används personliga inloggningsuppgifter. Detta leder till att användarna endast behöver logga ut från de applikationer som de loggat in på med sitt personliga användarnamn och lösenord. Respondent A ser inga fördelar med nuvarande autentiseringsmetod eftersom säkerhetsrisker kan uppstå:

> *”[…] Det är bara krångligt och onödigt egentligen men det är väl en följd av den utveckling som har varit, det är väldigt många system en del är gamla och en del är lite nyare det är inte så lätt att hålla det på en jämn nivå då. Att ha samma inloggning på allihop är det som man försöker åstadkomma nu framöver. Men då kräver det ombyggnad och förändring av en del system.”* – **Respondent A**

Respondent A anser även att risker kan uppstå med den nuvarande autentiseringsmetoden då användaren måste komma ihåg ett antal olika lösenord. Då det finns cirka 4500 anställda tror Respondent A att det förekommer att användaren skriver ner lösenord på papper och förvarar de nedskrivna lösenorden nära datorn. Enligt respondenten är detta en säkerhetsrisk då informationen kan utnyttjas av obehöriga användare. Enkätundersökningen på vårdcentralen i Mariestad visar att användarna har ett antal olika lösenord att komma ihåg. Det kan röra sig från allt mellan två till tio olika lösenord. Fördelningen mellan antalet lösenord bland de som besvarade enkäten såg ut följande:

Fråga 3: Hur många lösenord behöver du komma ihåg för att kunna utföra ditt arbete på din arbetsplats?

Antal lösenord	***Antal svar***	***Procentenheter***
2	1	7%

5	2	13%
5 - 6	1	7%
6	3	20%
8	4	27%
9	1	7%
10	3	20%

Tabell 2: Antalet lösenord per respondent.

Tabell 2 visar att en majoritet av användarna har mellan 5 och tio olika lösenord och detta innebär att användaren i många fall har svårt att memorera de olika lösenorden. Enkätundersökningen visar även att samtliga respondenter skriver ner sina lösenord för att lättare komma ihåg dem:

Fråga 7: Har du någon gång skrivit ner lösenord på t.ex. en papperslapp?

Ja	***Nej***
15	0
100%	0%

Tabell 3: Antalet respondenter som skriver ner sina lösenord.

Tabell 3 visar att antalet användare som skriver ner sina lösenord är många. I enkätundersökningen framgår det även att respondenterna tycker att det krävs för många inloggningar för att utföra det dagliga arbetet. Men de ser även det kontinuerliga utbytet av lösenord som ett problem då de måste memorera ett nytt lösenord. Många av respondenterna väljer därav att skriva ned lösenorden på papper. En av respondenterna skrev följande:

> *”För mycket inloggningar. Krångligt med byten av lösenord var 3:e månad.”*

Alla respondenter som deltagit i enkätundersökningen framhåller att de måste göra ett antal olika inloggningar för att utföra det dagliga arbetet. Majoriteten av respondenterna ger uttryck för att den nuvarande autentiseringsmetoden minskar flexibiliteten då de olika inloggningarna är tidskrävande. Respondenterna ger även uttryck för en önskan om förändring av den nuvarande autentiseringsmetoden:

> *”Behöver förändras. Tar mycket tid, ibland får dataansvarig tillkallas då man glömt bort lösenord”*

Även Respondent A anser att effektiviteten minskar och att administrationen kring lösenordshanteringen ökar med den nuvarande metoden:

> *”[…] inte lika effektivt så som det vore om man hade ett lösenord. […] det finns risker, det är inte effektivt och det är en väldig administration kring det också så som att uppdatera databaser med olika inloggningsuppgifter för varje system och det är ett väldigt jobb kring det, det är det ju.” –* **Respondent A**

5.2 Tankar kring Single Sign-On

Syftet med SSO är att underlätta och effektivisera arbetet samt att användarna inte ska behöva upprepa sin inloggning. Syftet är också att underlätta det dagliga arbetet då användarna slipper komma ihåg ett antal olika lösenord. Fördelarna är många och Respondent A ser inga nackdelar utan han anser att det kommer att bli enklare:

> *”Nej jag kan inte se några speciella nackdelar utan det blir enkelt” –* **Respondent A**

Syftet är att KSS i framtiden inte ska använda sig av användarnamn och lösenord i samma utsträckning som de gör idag. KSS vill därför gå över till användningen av smarta kort. Respondent B anser att den första utmaningen för att uppnå en Single Sign-On är att användarna måste kunna identifiera sig på ett säkert sätt:

> *”[…] det finns ju en del utmaningar och om vi börjar med den första utmaningen så är det ju så att om du ska ha en Single Sign-On så måste du veta vem det är som signar on, alltså du måste vara väldigt säker på individen. Om du ska ge dig på vården så har de krav på en väldigt säker identifiering. Det är till och med krav på att den ska vara så säker att det måste vara en två-faktorsautentisering” –* **Respondent B**

Idag finns det ett flertal olika system. Enligt Respondent A finns det flera hundra olika system och varje system har sin egen inloggning. SSO medför många fördelar där bland annat produktiviteten ökar då användarna slipper lägga ner tid på att logga in på olika system, vilket också är tidskrävande och frustrerande för användaren. Säkerheten ökar då användaren inte behöver komma ihåg ett antal olika användarnamn och lösenord, men med förutsättningen att två-faktorsautentisering används. Detta leder även till att lösenordrelaterade problem minskar. Det är även viktigt att nämna att det administrativa arbetet minskar då administratörer slipper lägga upp ett konto i varje system, och samma förfarande gäller vid bortagande av konton. För att lösa detta krävs en central användarhantering, men eftersom antalet system är många försvårar det införandet av en sådan. Respondent A ser inte detta som någon utmaning utan snarare som en större arbetsinsats som kommer att ta lite tid:

> *” […] det är en väldig flora av system så att säga bara mängden i sig gör ju att […] jag ser inte det som problem det är mer en större arbetsinsats som kommer att ta lite tid” –* **Respondent A**

Enkätundersökningen visar att majoriteten av användarnas arbete hade underlättats om de endast hade behövt logga in en gång och därefter kunnat komma åt alla andra system. Detta innebär att användarna helst vill ha ett användarnamn och ett lösenord för samtliga system (se tabell 4 och 5).

Fråga 11: Hade ditt arbete förenklats ifall du kunde komma åt alla system du har rättigheter till genom endast en inloggning?

Ja	***Nej***	***Vet inte***
14	0	1
93%	0%	7%

Tabell 4: majoriteten av respondenterna vill ha en SSO-lösning.

Fråga 12: Hade ditt arbete förenklats ifall du endast behövde komma ihåg ett lösenord för att logga in mot ett system och att du därefter kan komma åt alla system utan att upprepa din inloggning på nytt.

Ja	***Nej***	***Vet inte***
14	0	1
93%	0%	7%

Tabell 5: Enligt respondenterna hade arbetet förenklats ifall de endast hade behövt komma ihåg ett lösenord.

5.3 Tankar kring två-faktorsautentisering

För att möjliggöra SSO är det ett krav att användarna kan identifiera sig. Kraven är så pass höga att det krävs två-faktorsautentisering. SITHS är en del av den tekniska infrastrukturen som ingår i den Nationella IT-strategin och är en säkerhetslösning för elektronisk identifiering. Eftersom kraven på säkerhet är höga inom hälso- och sjukvården räcker det inte med endast mjuka certifikat, utan ett PKI-certifikat måste förvaras på ett smart kort. SITHS kan möjliggöra följande (Näsberg, 2010):

- Tillföra den säkerhet som krävs för Single Sign-On.
- Digitalt signerade recept, journalhandlingar med mera.
- Säker e-post med identifikation av avsändare.
- Säker överföring av medicinsk information.

Med SITHS-kortet kan en användare identifiera och ge bevis för sin behörighet. Det förenklar bland annat in- och utloggningen till olika datasystem då användaren endast behöver logga in en gång med ett enda lösenord. Enligt Respondent A används kortet redan idag som passerkort till olika lokaler. Tanken är att kortet ska användas till andra tjänster och inte bara för inloggning till datasystem. Kortet ska till exempel användas för att öppna dörrar, utföra digitala signaturer och kryptera information:

> *”[…] det är redan igång med för att komma in till huset. Det ska vara många funktioner på det och inte bara till datasystem det är ett passerkort och en ID-handling kan man säga så den ska du bära på dig hela tiden.” –* **Respondent A**

SITHS-lösningen bygger på att de anställda får tillgång till ett personligt ID-kort med elektroniska legitimationer som möjliggör en säker identifiering och kryptering av känslig information (Carelink).

Ett problem som återstår att lösa, enligt Respondent A, är det som sker efter att en användare drar ut sitt kort från kortläsaren vid ett avbrott av arbetet. Det är oklart vad som sker med sessionen före avbrottet då användaren loggar in på samma eller någon annan arbetsstation. Enligt Respondent A ska inte användaren behöva starta om alla applikationer utan användaren ska kunna dra ut sitt kort när som helst och när denne loggar in på samma eller någon annan arbetsstation vid ett senare tillfälle komma tillbaka till samma session där denne var innan avbrottet:

> *”[…] vad händer om du ska skriva lite grann och sen ska du gå därifrån drar du ut ditt kort vad händer då liksom sen kommer nästa och vad händer med sessionen o det finns en del grejer att fundera på där men jag tror det går att lösa och så men jag tror det är ett stort arbete som kvarstår.”* – **Respondent A**

Vidare menar Respondent A att detta problem är viktigt att lösa då det kan hända att vårdpersonalen samlar på sig dokumentation till slutet av dagen. Tanken är att personalen ska kunna logga in på vilken dator som helst och när som helst för att avsluta det påbörjade arbetet trots fysiska förflyttningar. Detta skulle innebära att användarna slipper samla på sig dokumentation till slutet av dagen och istället ges möjligheten till att dokumentera under dagen. Enligt Respondent A är detta en ytterst viktig del inom hälso- och sjukvården då information ska vara korrekt. För att förenkla användarens arbete och öka tillgängligheten ska användarna kunna logga in på flera olika arbetsstationer och fortsätta sitt arbete där de senast avslutade det. För att lösa detta krävs en förändring av PC-miljön. I Karlstad kommun har man löst detta genom att flytta datorn till ett centralt serverrum och istället använda sig av tunna klienter (se avsnitt 2.9.1).

6 Slutsats

I det här avsnittet dras slutsatser av studien och det jag kommit fram till utifrån resultatet. Uppsatsens forskningsfråga lyder som följer:

- *Vilka eventuella utmaningar samt möjligheter ges vid införandet av SSO och Två-faktorsautentisering i förhållande till nuvarande autentiseringsmetod?*

För att göra slutsatserna överskådliga har jag valt att dela upp forskningsfrågan i två delfrågor. Frågorna besvaras i avsnitt 6.1 respektive 6.2.

- *Vilka **möjligheter** ges vid införandet av SSO och Två-faktorsautentisering i förhållande till nuvarande autentisering?*

- *Vilka **utmaningar** tros man stöta på vid införande av SSO och Två-faktorsautentisering?*

6.1 Vilka möjligheter ges vid införandet av SSO och Två-faktorsautentisering i förhållande till nuvarande autentisering

I dagsläget använder sig KSS av lösenord som autentiseringsmetod och en SSO-lösning. Med utgångspunkt i resultatet kan det konstateras att en SSO-lösning är svår att implementera då hundratals olika system används. KSS använder en så kallad gruppinloggning där ett antal olika användare har ett gemensamt användarnamn och lösenord till klientdatorn, men användarna har personliga användarnamn och lösenord då de till exempel ska läsa eller skriva i journalsystem.

Då KSS inte har en SSO-lösning kan man utifrån resultatet konstatera att användarna måste komma ihåg ett antal olika lösenord. Enkätundersökningen visar att det förekommer att användaren inte loggar ut från system då de ska göra ett kortare avbrott eller att de skriver ner, lånar ut och lånar lösenord från arbetskamrater. Detta leder till att säkerhetsrisker uppstår då obehöriga lättare kan få tillgång till information de inte ska ha tillgång till. Ytterligare en slutsats som kan dras från enkätundersökningen är att den nuvarande autentiseringsmetoden är tidskrävande och ineffektiv då användarna måste logga in på ett antal olika system/applikationer med olika lösenord.

6.1.1 Förenklade arbetsrutiner

SSO förenklar det dagliga arbetet för vårdpersonalen då de inte behöver komma ihåg ett antal olika lösenord för att utföra det dagliga arbetet. Genom det Personliga SITHS-kortet med tillhörande PIN-kod behöver användaren endast logga in en gång och därefter får de tillgång till de tjänster de har rättigheter till utan ytterligare inloggningar.

Det är inte bara användarnas arbete som skulle underlättas vid införandet av SSO. Även det administrativa arbetet förenklas då administratörer inte behöver skapa ett konto i varje system, och samma förfarande gäller vid borttagande av konto.

6.1.2 Säkrare autentisering

Eftersom det finns krav på stark autentisering inom hälso- och sjukvården är autentisering med hjälp av endast lösenord för svagt. De möjligheter som ges med SSO tillsammans med två-faktorsautentisering är en lösning som skulle uppfylla säkerhetskraven som hälso- och sjukvården efterfrågar. Med två-faktorsautentisering minskar riskern att obehöriga får tillgång till känslig information. Även användarnas krav på enkelhet och effektivisering av inloggningsrutiner förenklas, då användaren endast behöver komma ihåg ett lösenord och endast logga in en gång för att komma åt önskade system. Därmed är det troligt att risken att användaren skriver ner eller återanvänder gamla lösenord minskar.

6.1.3 Ökad säkerhet

Eftersom det är viktigt att känslig patient information inte hamnar i orätta händer är det viktigt med stark autentisering. Eftersom användarna inte behöver komma ihåg ett antal olika lösenord är det troligt att risker minskar att användarna skriver ner eller återanvänder gamla lösenord. Med tanke på användaren inte behöver memorera ett antal olika lösenord då en SSO-lösning finns är det ytterst viktigt att det personliga SITHS-kortet alltid skall finnas till hands. SITHS-kortet är ett multifunktionellt kort vilket innebär att användaren bland annat måste ha kortet till inloggning mot system eller som ett passerkort. Detta medför troligtvis att användaren är mer rädd om SITHS-kortet då det är mer personligt. Risken att användaren lämnar kvar kortet i kortläsaren vid kortare avbrott eller lånar ut sitt kort till arbetskamrater minskar troligtvis.

6.2 Vilka eventuella utmaningar tros man stöta på vid införandet av SSO och Två-faktorsautentisering?

6.2.1 En uppsjö av olika system

KSS är i planeringsfasen av införandet av en SSO-lösning och en så kallad två-faktorsautentisering, vilket intervjupersonerna anser är den största utmaningen. Det är svårt att implementera en SSO-lösning med tanke på att KSS har ett hundratal olika verksamhetssystem. Varje system har sin egna roll- och behörighetshantering. Detta ses inte som ett problem utan som en större utmaning som kommer att kräva en större arbetsinsats. För att underlätta arbetet ska viktigare system sättas i drift först och därefter anpassas mindre system i samma kedja.

6.2.2 Sessionåterupptagning

En annan utmaning är hanteringen av sessioner då användare väljer att dra ut SITHS-kortet. Att komma på en bra lösning är en utmaning. Detta är viktigt då vårdpersonalen i nuläget samlar på sig information till slutet av dagen innan systemen uppdateras med den nya informationen. Karlstads kommun har löst sessionåterupptagningen med hjälp av ”Smart arbetsplats” som bygger på terminalserverfunktionalitet. För att komma fram till en bra lösning vad gäller SSO, två-faktorsautentisering och sessionåterupptagning krävs noggrann planering och stor en arbetsinsats.

7 Diskussion

I detta avsnitt diskuteras resultatet av föreliggande studie och den valda metoden som tillämpats för att besvara studiens forskningsfrågor.

7.1 Diskussion av resultatet

Syftet med rapporten var att undersöka eventuella utmaningar samt möjligheter som ges vid införandet av SSO och två-faktorsautentisering i förhållande till den nuvarande autentiseringsmetoden. Genom kvalitativa semistrukturerade intervjuer, semistrukturerade enkätfrågor men även genom litteraturstudier ville jag ge svar på rapportens forskningsfråga:

- *Vilka eventuella utmaningar samt möjligheter ges vid införandet av SSO och Två-faktorsautentisering i förhållande till nuvarande autentiseringsmetod?*

Resultatet av denna studie visar att en SSO-lösning tillsammans med en två-faktorsautentisering är det som krävs för att uppfylla de krav som ställs inom hälso- och sjukvården. Säkerhetskraven uppfylls men även det dagliga arbetet för vårdpersonalen förenklas då de inte behöver komma ihåg ett flertal olika lösenord.

Hälso- och sjukvården har höga krav på rutiner kring säkerhet och åtkomst av information. Vidare finns det strikta bestämmelser om loggning av händelser i syfte att förebygga obehörig åtkomst (SFS, 2008:355). Med utgångspunkt i patientdatalagen anser jag att SSO-lösningen tillsammans med två-faktorsautentisering uppfyller de säkerhetskrav som ställs på hälso- och sjukvården (till exempel stark autentisering). Vidare anser jag att en SSO-lösning med två-faktorsautentisering underläter vårdpersonalens vardagliga arbete (t.ex. enklare inloggningar) samtidigt har säkerheten höjs.

Att ha en inloggning till alla system med endast ett lösenord löser inte de säkerhetskrav som ställs inom hälso- och sjukvården. Istället är en två-faktorsautentisering ett måste för att uppfylla kraven på stark autentisering. Enkätundersökningen visar att det förekommer att vårdpersonalen lånar lösenord av varandra. Det är troligt att denna problematik inte kommer att lösas med hjälp av en två-faktorsautentisering. Även ett SITHS-kort med tillhörande lösenord kan lånas ut till kollegor. För att förhindra utlåningen av SITHS-korten anser jag att det är ytterst viktigt med utbildning och information om IT-säkerhet. Det är viktigt att lyfta fram varför kort/lösenord inte ska lånas ut, det är viktigt att påpeka att allt som görs på ett system loggas. Detta för att användaren ska ha klart för sig att de inte kan göra vad de vill utan att någon ser. Jag anser även att det är viktigt att påpeka konsekvenserna av att låna ut korten till obehöriga, det vill säga personliga konsekvenser i form av varningar och indrag av legitimation och så vidare. Det är minst lika viktigt att informera om konsekvenserna av utlåningen som kan drabba patienterna, eftersom obehöriga då kan ta del av känslig och sekretessbelagd information. Även en ökad kontroll av loggning är ett måste för att på bästa sätt förhindra att kort lånas ut eller att ett kort/inloggning används under en hel arbetsdag. Genom att binda fler funktioner till SITHS-kortet anser jag att kortet blir mer personligt och kan därför förhindra att användarna lånar ut sina kort till varandra. Genom att till exempel använda kortet som passerkort till olika lokaler minskar risken att användaren lånar ut sitt kort då SITHS-kortet behövs för att förflytta sig.

7.2 Metoddiskussion

Jag valde att använda mig av två metoder för datainsamling, d.v.s. en primär och en sekundär datainsamlingsmetod. I den primära datainsamlingsmetoden användes kvalitativa semistrukturerade intervjuer och semistrukturerade enkätfrågor. I den sekundära datainsamlingsmetoden använde jag mig av litteraturstudier för att få tag på relevant information.

För att svara på rapportens forskningsfråga ansåg jag att den primära datainsamlingsmetoden skulle ligga till grund för rapportens resultat medan den sekundära datainsamlingsmetoden skulle ligga till grund för rapportens bakgrund. Jag är nöjd med valen av datainsamlingsmetoder men självklart fanns det för- och nackdelar med respektive metod. Den primära metoden var tidskrävande då det krävdes mycket för- och efterarbete. Andra problem som jag stötte på med den primära metoden var att jag inte fick tag på de personer som jag ville få tag på. Jag fick endast göra en intervju med en IT-strateg från KSS och med tanke på att rapporten avgränsades till KSS var detta en stor motgång för mig. Andra problem som jag stötte på med den primära datainsamlingsmetoden var att jag väldigt sent blev informerad om att jag inte fick dela ut enkäterna till vårdpersonalen på KSS. Istället fick jag söka mig till vårdcentralen i Mariestad. Efter att jag tagit kontakt med informationsansvarig på vårdcentralen förklarade jag syftet med enkätundersökningen men även att insamlingen av enkäterna skulle ske efter en vecka. Även här stötte jag på problem då jag inte kunde göra min enkätinsamling förrän cirka en månad efter att de delats ut.

Den sekundära datainsamlingsmetoden använde jag för att få bakgrundsinformation. Eftersom problemen med ineffektiva inloggningsrutiner, lösenordhantering men också de krav som ställts på hälso- och sjukvården för stark autentisering redan finns dokumenterade ansåg jag att en litteraturstudie var passande för rapporten. Eftersom det fanns relevant material både i tryckt och elektroniskt format underlättades arbetet. Det var dock svårt att hitta forskningsartiklar och andra former av dokument som har studerat möjligheter och utmaningar med SSO och två-faktorsautentisering. Därför var det lämpligt att använda den kvalitativa forskningsintervjun för att kunna besvara studiens forskningsfråga. Om endast en litteraturstudie hade genomförts hade det varit svårt att besvara rapportens forskningsfråga.

7.3 Framtida arbete

Allt fler landsting ansluter sig till HSA, men det finns ett flertal olika sätt att ansluta sig till HSA (se avsnitt 2.8). Jag anser därför är det ett relevant forskningsområde, d.v.s. att närmare forska kring de olika metoderna som landstingen väljer. Att jämföra de olika anslutningsmetoderna och undersöka för- och nackdelar med respektive metod är relevant för utvecklingen inom sjukvården.

8 Referenser

Bell, J. (1995). *Introduktion till forskningsmetodik* (2:a upplagan). Lund: Studentlitteratur.

Carling, M. (2007). *Rätt kort ger smart inloggning*. Tech world. Tillgänglig på Internet: http://sakerhet.idg.se/2.1070/1.95298 [Hämtad: 10.04.05].

Dahlberg, K. (1997). *Kvalitativa metoder för vårdvetare* (2:a upplagan). Lund: Studentlitteratur.

Datainspektionen. Patientdatalagen. Tillgänglig på Internet: http://www.datainspektionen.se/fragor-och-svar/faq-patientdatalagen/ [Hämtad: 10.08.19].

Denscombe, Martyn (2000). *Forskningshandboken: för småskaliga forskningsprojekt inom samhällsvetenskaperna*. Lund: Studentlitteratur

Fredriksson, S. (2008). *Logica vann bif-upphandling*. It-vården. Tillgänglig på Internet: http://itivarden.idg.se/2.2898/1.155716 [2010.04.19]

Gravin, K. (2008). *HSA-katalog*. Kommunförbundet Skåne. Tillgänglig på Internet: http://www.kfsk.se/sidor/verksamheter/vardomsorgochsocialafragor/itivardochomsorg/hsakatalog.267.html [2010.05.01].

Inera, (2010). SITHS – ett säkert kort. *Smart arbetsplats, mindre krångel och mer fokus på vården.* Inera AB. Tillgänglig på Internet: http://www.inera.se/VirtDocRoot%5CTj%C3%A4nster%5CSITHS%5CVisas%20p%C3%A5%20bolagswebb/01.%20Informationsmaterial/SITHS-broschyr_April%202010t.pdf [2010.06.13].

Johansson, L. (2009). *RIV Informationsspecifikation: verksamhetsdokumentation för HSA Struktur och innehåll.* Sjukvårdsrådgivningen. Tillgänglig på Internet: http://avtal.skane.se/HolgerDokument/09/02273/Bilaga15RIVInformationsspecifHSA.pdf [2010.05.01]

Johansson, L. *HSA Nationell Katalogtjänst: gemensam nationell informationskälla för kvalitetssäkrade uppgifter om personer, enheter och funktioner*. Sjukvårdsrådgivningen. Tillgänglig på Internet: http://www.carelink.se/dokument/forvaltning_och_tjanster/hsa/HSA_Nationell_Katalogtjanst_2009-09-10.pdf [2010.05.01].

Loshin, P. (2001). *Single sing-on*. Computerworld, *6*, pp. 64-65.

Medin, A. (2010). *Journalportal breddinförande*. Landstinget i Östergötland. Tillgänglig på Internet: http://www.lio.se/Verksamheter/Vardprocesscentrum/Projektstyrning/Projektlista/Pagaende-projekt/Journalportal-breddinforande/ [2010.06.17].

Mitrovic, P. (2003). *IT-säkerhet* (3:e upplagan). Pagina Förlags AB.

Mitovic, P. (2005). *IT-säkerhet* (4:e upplagan). Pagina Förlags AB.

Neuman, B. C. och Ts'o, T. (1994). *Kerberos: authentication service for computer networks.* Institute of Electrical and Electronics Engineers. Tillgänglig på Internet: http://gost.isi.edu/publications/kerberos-neuman-tso.html [Hämtad: 10.02.22].

Nilsson, J. (2008). *Informationssäkerhet stort problem inom vården.* IT i vården. Tillgänglig på Internet: http://itivarden.idg.se/2.2898/1.155154 [Hämtad: 10.02.22]

Näsberg, T. (2010). *SITHS – säker it i hälso och sjukvården.* Center för eHälsa i samverkan. Tillgänglig på Internet: http://www.cehis.se/infrastruktur/siths/ [Hämtad: 10.05.27].

Ricknäs, M. (2004). *Säkerheten är en knäckfråga.* Computer Sweden. Tillgänglig på Internet: http://computersweden.idg.se/2.2683/1.24165 [Hämtad: 10.02.22].

Schneier, B. (1998). *Biometrics: truths and fictions*. Counterpane systems. Tillgänglig på Internet: http://www.schneier.com/crypto-gram-9808.html [Hämtad: 10.04.03].

Stamp, M. (2006). *Information security: principles and practice.* Hoboken, NJ, USA: John Wiley & Sons, Inc.

Starrin, Bengt & Svensson, Per-Gunnar (red.) (1994). *Kvalitativ metod och vetenskapsteori*. Lund: Studentlitteratur

Westerlund, K. (2008). *Många använder enkla lösenord*. Dagens nyheter. Tillgänglig på Internet: http://www.dn.se/ekonomi/manga-anvander-enkla-losenord-1.594700 [2010.08.08].

Williams, R. (2000). *Kerberos explained*. Microsoft Corporation. Tillgänglig på Internet: http://technet.microsoft.com/en-us/library/bb742516.aspx [Hämtad: 10.01.25].

Östnäs, M. (2010). *Sjuksköterska får dagsböter för att ha tjuvläst journal.* IT i vården. Tillgänglig på Internet: http://itivarden.idg.se/2.2898/1.330031/sjukskoterska-far-dagsboter-for-att-ha-tjuvlast-journal [Hämtad: 10.08.15].

Bilaga A - Enkätundersökning

1: Hur gammal är du?

18 – 25	26 – 35	36 – 45	46 – 55	56 – 65

2: Hur ofta använder du en dator på din arbetsplats?

Varje dag	Någon gång i veckan	Nästan aldrig	Aldrig

3: Hur många lösenord behöver du komma ihåg för att kunna utföra ditt arbete på din arbetsplats?

Antal lösenord: ____

4: Är du nöjd med nuvarande inloggningsprocess som krävs för att utföra det dagliga arbetet?

(Med inloggningsprocess menas t.ex. att uppge användarnamn och lösenord)

Ja	Nej

Egna åsikter:

Om nej på frågan ovan, varför?

5: Behöver du logga in på flera olika system för att komma åt informationen du behöver för att utföra dina arbetsuppgifter?

Ja	Nej

Egna åsikter:

Om ja på frågan ovan, tycker du att detta borde förändras och varför?

6: Anser du att nuvarande inloggningsprocess är ett hinder för att göra ditt arbete effektivt?

Ja	Nej

Egna åsikter:

Om ja på frågan ovan, varför?

Informationssäkerhet

7: Har du någon gång skrivit ner lösenord på t.ex. en papperslapp?

Ja	Nej

8: Har du någon gång lånat ut dina inloggningsuppgifter till någon?

Ja	Nej

8a: Om ja till vem/vilken situation:

- ☐ Till arbetskamrat
- ☐ Till vikarie
- ☐ Vid sjukdom
- ☐ Annan: _____

9: Har du någon gång lånat inloggningsuppgifter av någon?

Ja	Nej

9a: Om ja, av vem/vilken situation:

- ☐ Av arbetskamrat
- ☐ Vid vikarie
- ☐ Annan: _____

10: Loggar du ut från datorn när du till exempel går på lunch eller av annan anledning måste lämna datorn för en stund?

Alltid	Ibland	Aldrig

10a: Om ibland och aldrig varför?

- ☐ Tidsbrist
- ☐ Glömmer
- ☐ Inget säkerhetshot uppstår
- ☐ Annan orsak: _____

Övriga frågor

11: Hade ditt arbete förenklats ifall du kunde komma åt alla system du har rättigheter till genom endast en inloggning?

Ja	Nej	Vet inte

12: Hade ditt arbete förenklats ifall du endast behövde komma ihåg ett lösenord för att logga in mot ett system och att du därefter kan komma åt alla system utan att upprepa din inloggning på nytt.

Ja	Nej	Vet inte

13: Hade du föredragit att använda ett personligt kort (Smarta kort) tillsammans med en PIN-kod som inloggningsmetod istället för nuvarande inloggningsmetod.
(Personligt kort + PIN-kod fungerar som bankomatkort. För att logga in på systemet sätter du in ditt personliga kort i en kortläsare och därefter skriver du in din PIN-kod).

Ja	Nej	Vet inte

Bilaga B - Sammanställning av enkätsvaren

1: Hur gammal är du?

18 – 25	**26 – 35**	**36 – 45**	**46 – 55**	**56 – 65**
0	3	5	7	0
0%	20%	33%	47%	0%

2: Hur ofta använder du en dator på din arbetsplats?

Varje dag	**Någon gång i veckan**	**Nästan aldrig**	**Aldrig**
15	0	0	0
100%	0%	0%	0%

3: Hur många lösenord behöver du komma ihåg för att kunna utföra ditt arbete på din arbetsplats?

Antal lösenord	**Antal svar**	**I procent**
2	1	7%
5	2	13%
5 - 6	1	7%
6	3	20%
8	4	27%
9	1	7%
10	3	20%

4: Är du nöjd med nuvarande inloggningsprocess som krävs för att utföra det dagliga arbetet?

(Med inloggningsprocess menas t.ex. att uppge användarnamn och lösenord)

Ja	**Nej**
10	5
67%	33%

Egna åsikter:

- *”För många olika lösenord”*
- *”Logga in på flera ställen tar mycket tid”*
- *”För mycket inloggningar. Krångligt med byten av lösenord var 3:e månad”*

5: Behöver du logga in på flera olika system för att komma åt informationen du behöver för att utföra dina arbetsuppgifter?

Ja	**Nej**
15	0
100%	0%

Egna åsikter:

- *”Ja, för att det ska bli smidigare, och spara tid.”*
- *”Det vore skönt att slippa logga in på så många olika ställen men jag har svårt att se hur vi kan slippa när det är olika system.”*
- *”Näe, det är väl inte så mycket att göra åt.”*
- *”Nej det är bra.”*
- *”Ju färre system desto bättre.”*
- *”Tidstjuv.”*
- *”Har ej funderat på det, det är ju olika system program och kan väl inte fungera annars.”*
- *”Behöver förändras – tar mycket tid, ibland får dataansvarig tillkallas då man glömt lösenord.”*

6: Anser du att nuvarande inloggningsprocess är ett hinder för att göra ditt arbete effektivt?

Ja	**Nej**
5	10
33%	67%

Egna åsikter:

- *”För många olika inloggningar.”*
- *”Ibland tar tid!”*
- *”Kan trassla och ta tid om man glömmer lösenord. Då det är många att komma ihåg.”*

7: Har du någon gång skrivit ner lösenord på t.ex. en papperslapp?

Ja	**Nej**
15	0
100%	0%

8: Har du någon gång lånat ut dina inloggningsuppgifter till någon?

Ja	**Nej**
6	9
40%	60%

8a: Om ja till vem/vilken situation:

Svarsalternativ	***Svar***
Till arbetskamrat	5
Vid vikarie	1
Vid sjukdom	0
Annan	1

(**OBS!** En respondent har svarat på två alternativ: arbetskamrat och annan).

9: Har du någon gång lånat inloggningsuppgifter av någon?

Ja	**Nej**
9	6
60%	40%

9a: Om ja, av vem/vilken situation:

Svarsalternativ	***Svar***	***I procent***
Av arbetskamrat	7	78%
Vid vikarie	2	22%
Annan	0	0%

10: Loggar du ut från datorn när du till exempel går på lunch eller av annan anledning måste lämna datorn för en stund?

Alltid	**Ibland**	**Aldrig**
8	7	0
53%	47%	0%

10a: Om ibland och aldrig varför?

Svarsalternativ	***Svar***	***I procent***
Tidsbrist	2	29%
Glömmer	3	43%
Inget säkerhetshot uppstår	1	14%
Annan orsak	1	14%

11: Hade ditt arbete förenklats ifall du kunde komma åt alla system du har rättigheter till genom endast en inloggning?

Ja	**Nej**	**Vet inte**
14	0	1
93%	0%	7%

12: Hade ditt arbete förenklats ifall du endast behövde komma ihåg ett lösenord för att logga in mot ett system och att du därefter kan komma åt alla system utan att upprepa din inloggning på nytt.

Ja	**Nej**	**Vet inte**
15	0	0
100%	0%	0%

13: Hade du föredragit att använda ett personligt kort (Smarta kort) tillsammans med en PIN-kod som inloggningsmetod istället för nuvarande inloggningsmetod.
(Personligt kort + PIN-kod fungerar som bankomatkort. För att logga in på systemet sätter du in ditt personliga kort i en kortläsare och därefter skriver du in din PIN-kod).

Ja	**Nej**	**Vet inte**
6	0	9
40%	0%	60%

Bilaga C - E-mailutskick till landsting och kommuner

Hej,
Mitt namn är Besart Rexhepi. Jag är studerande på Högskolan i Skövde och skriver för tillfället mitt examensarbete inom Datalogi.

Jag har valt att skriva om Single Sign-On och två-faktorsautentisering (SITHS) inom Hälso- och Sjukvården.

Mina frågor till Er är:

- Hur långt ni har kommit i arbetet när det gäller Single Sign-On och SITHS?
- Använder ni er av SITHS-kort för autentisering?
- Har ni någon Single Sign-On-lösning där användaren kan komma åt flera system utan att behöva upprepa sin inloggning?
- Karlstad kommun har löst frågorna ovan med hjälp av något som de kallar för Smarta arbetsplatser. Hur ser det ut hos er? Har ni någon Single Sign-On-lösning och använder ni er av SITHS-kort?

Jag är tacksam om jag kunde få lite information om hur det ser ut hos er.

Tack på förhand!
Mvh
Besart Rexhepi