IT University of Göteborg
CHALMERS | GÖTEBORG UNIVERSITY

Kandidatuppsats i informatik
Thesis work in Informatics

REPORT NO. 2008:046
ISSN: 1651-4769

Instutitionen för tillämpad IT
Department of Applied Information Technology

En studie i användandet av Single Sign-On inom offentlig sektor

A study in the use of Single Sign-On in Swedish public sector

FREDRIK AHLBORG
JOHNNY HÅLSJÖ

CHALMERS | UNIVERSITY OF GOTHENBURG

IT University of Göteborg
Chalmers University of Technology and University of Gothenburg
Göteborg, Sweden 2008

Abstrakt

Idag använder verksamheter sig av en mängd olika applikationer och system. Dessa kräver olika typer av behörighet, beroende på vilken befattning användaren innehar i verksamheten. Det traditionella sättet för att autentisera sig i dessa system är att använda sig av användarnamn och lösenord. Allt eftersom fler system utvecklas och införskaffas måste användaren komma ihåg flera lösenord. Single Sign-On är en teknik för att underlätta inloggning vid flera system, då användaren enbart behöver logga in en gång.

Syftet med uppsatsen var att undersöka användandet av Single Sign-On inom offentlig sektor. Uppsatsens frågeställning lydde enligt följande: *Vilka aspekter bör beaktas vid användandet av Single Sign-On inom offentlig sektor?*

Studien har genomförts med en hermeneutisk prägel och vi använt oss av en kvalitativ forskningsmetod. Den kvalitativa forskningsmetoden har bestått av semistrukturerade intervjuer och har omfattat sex respondenter. Studien har genomförts i Göteborgsregionen och omfattat tre kommuner. I varje kommun bestod respondenterna av en med god kännedom om IT-verksamhet och en med god insyn i helpdesk-verksamheten.

Resultatet av studien visade att vi identifierade en centraliserad och decentraliserad lösenordshantering. Vi identifierade följande aspekter: *ekonomiska, organisatoriska, säkerhetsmässiga* och *tekniska*.

Nyckelord: användarhantering, centraliserad, decentraliserad, offentlig sektor,
Single Sign-On.

Handledare: Alan B Carlsson

Tack

Stort tack till alla respondenterna som ställt upp tålmodigt och svarat på våra undersökande frågor och som gjort denna rapport möjlig. Vi vill även rikta ett tack till de som korrekturläst vår uppsats och bidragit med respons. Avslutningsvis vill vi tacka vår handledare, Alan B Carlsson, som bidragit med tips och idéer.

Fredrik Ahlborg och Johnny Hålsjö, maj 2008

Innehållsförteckning

1. Introduktion

Många verksamheter använder sig idag av en mängd olika applikationer och system. Dessa kräver olika typer av behörighet beroende på vilken befattning användaren innehar i verksamheten. Det traditionella sättet för autentisering i dessa system är att använda sig av användarnamn och lösenord. Allt eftersom fler system utvecklas och införskaffas måste användaren komma ihåg fler lösenord. En högkonsumerande användare av IT-system använder idag närmare 20 lösenord och för några enstaka användare kan antalet lösenord uppgå till över 50 (Hayday, 2002). Detta resulterar i att de olika organisationernas helpdesk får allt fler lösenordsrelaterade supportsamtal och kostnaden för dessa kan, enligt Hayday (2003), uppgå till 25$ per samtal (motsvarande 150-200 kr). Anställda tenderar att välja enklare lösenord, då den anställde behöver komma ihåg allt fler lösenord (Kotadia, 2004).

För att förhindra enklare lösenord bygger man ofta in system som kräver fler tecken i lösenordet. Detta resulterar istället att de anställda antingen börjar anteckna lösenord och förvarar dessa i anknytning till datorn, eller använder samma lösenord i flera system (Kotadia, 2004). I en del verksamheter ställs inte heller kravet på att användaren måste byta lösenord inom en viss tid, vilket leder till att kan använda samma under längre perioder. Gartner (Allan, 2007) hävdar att samma lösenord kan komma att användas upp till 7 år. Det finns även exempel på system som inte alls har någon kontroll av lösenordet och lösenordet kan i värsta fall vara samma som användarnamnet. Ett känt fall var folkparitets intrång i socialdemokraternas interna nätverk Sapnet, där en användare använde sig av ”sigge” som både användarnamn och lösenord (Jeräng, 2007). Det finns även ett annat sätt att se problemet med användarhantering. Vid användandet av e-post, nyttjande av e-handel etc. krävs det oftast att användaren skapar ett användarkonto per webbplats. Konsekvenserna av detta blir att en användare har ett stort antal konton att administrera. Det har därför utvecklats tekniker för att underlätta hanteringen av kontoadministrationen på Internet. Dessa tekniker är bland annat e-legitimation och OpenID.

För att lösa dilemmat med lösenordshantering och samtidigt höja säkerheten har det utvecklats en teknik som kallas för Single Sign-On (SSO). Tekniken bygger på att en användare enbart loggar in en gång för att få tillgång till alla system som användaren har behörighet till. På så vis slipper användaren att logga in i varje system (Davida et al, 2002).

Detta som från början gick ut på att höja säkerheten leder snarare tvärtom, till att säkerheten minskar och åtkomsten till informationen för en utomstående ökar. Behovet av både fysisk, logisk och organisatorisk säkerhet ökar i dagens samhälle, då allt mer information lagras digitalt och enkelt kan spridas och orsaka stor skada för både organisationer och individer (Mitrović, 2005).

1.1 Syfte

Syftet med denna studie är att undersöka användandet av SSO inom offentlig sektor. Vi är intresserade av att få svar på följande fyra frågeställningar:
Vilka faktorer får en offentlig verksamhet att införa Single Sign-On?
Innebär Single Sign-On en ekonomisk nytta?
Vilka säkerhetsaspekter finns det i att använda Single Sign-On i affärskritiskverksamhet?
Hur kan en offentlig verksamhet tillgodose sig nyttan av OpenID?

1.2 Avgränsning och Huvudfråga

Vi har valt att avgränsa denna uppsats till att bara omfatta kommuner i vår geografiska närhet, vilket i denna forskningsstudie enbart berör kommuner i Göteborgsregionen.
Uppsatsen berör inte tekniska aspekter inom SSO, utan syftar till att undersöka användandet och de aspekter som förligger. Detta leder fram till uppsatsens frågeställning: *Vilka aspekter bör beaktas vid användandet av Single Sign-On inom offentlig sektor?*

1.3 Disposition

Vi har delat upp studien i följande avsnitt. Avsnitt 2 (Teoretiskt ramverk) innehåller det teoretiska ramverket som ligger till grund för vår studie. Avsnitt 3 (Metod) innehåller valet av forskningsmetod och tillvägagångssätt vid genomförandet av studien. Avsnitt 4 (Resultat & Analys) innehåller resultatet från vår studie och i avsnitt 5 (Diskussion) diskuteras resultatet. Studien avslutas med en slutsats i avsnitt 6 (Slutsats).

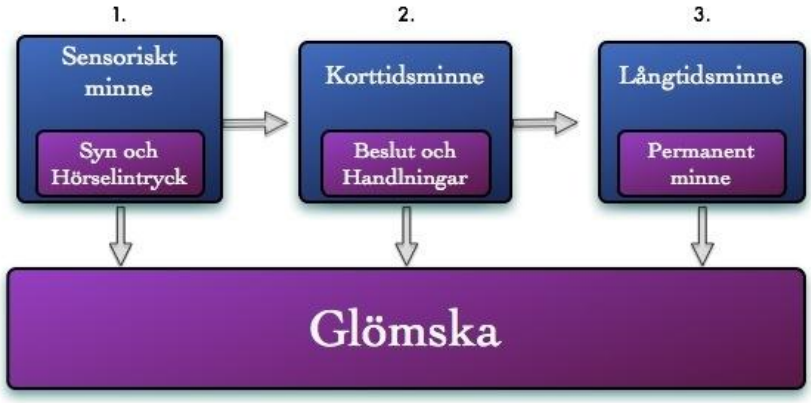
2. Teoretiskt ramverk

I detta avsnitt beskriver vi de teorier som framkommit genom vår litteraturstudie. Vi har delat in de i följande ämnen: Människans minnesförmåga, IT-säkerhet, Motivation, Offentlig sektor, Single Sign-On och Metakatalog

2.1 Människans minnesförmåga

Det finns en mängd samling teorier kring hur människans minnesförmåga fungerar. Vi har av förklarliga skäl inte hunnit ta del av alla dessa i vår litteraturstudie, utan valt att studera väletablerade minnesmodeller.

Människans minneskapacitet kan liknas vid hur en dators olika minnen fungerar. En dator består av primärminnet, alltså arbetsminnet och sekundärminnet, hårddisken, cd, USB-minne etc. Psykologerna Atkinsson & Shiffrin (1968) har utvecklat en modell kallad Multi-Store (figur 1) vilken beskriver de typer av minnesfunktioner hjärnan består av: sensoriska minnet, korttidsminnet och långtidsminnet (figur 1).



Figur 1- Det sensoriska minnet (1) intar syn- och hörselintryck en del förmedlas till korttidsminnet (2), som bearbetar och analyserar informationen och av detta förmedlas till långtidsminnet (3) som lagrar informationen permanent (Baserad på Atkinson & Shiffrains Multi-store modell 1968, s.113).

Denna modell har delvis blivit ifrågasatt när det gäller hur länge informationen behålls i korttidsminnet (Baddely, 1998). Det sensoriska minnet är det minne, som uppfattar vad sinnena såsom hörseln eller synen förmedlar. Sensoriska minnet är impulsstyrt och minns extremt korta perioder. Det handlar om intryck i upptill ett par sekunder och en del av dessa intryck skickas vidare till korttidsminnet (Atkinsson & Shiffrin, 1968).

Korttidsminnet eller arbetsminnet, som det också brukar kallas, är det minne som vi använder för synintryck och tankar i huvudet och som vi har för stunden, exempelvis vad nästkommande ord eller mening kommer att vara. Begränsningen av korttidsminnet har diskuterats flitigt och en av de mest ihärdiga forskarna inom området var George Miller. Det

är han som ligger bakom teorin *The Magical Number Seven, Plus or Minus Two*. Teorin går förenklat ut på att vi människor enbart kan minnas sju siffror eller bokstäver samtidigt. Betänk talet 823231418550145645152. Om du försöker minnas alla siffrorna kommer du enligt Millers teori enbart komma upp i runt sju siffror. Om du däremot delar upp siffrorna i grupper, såkallade chunks, kommer du att komma ihåg fler, exempelvis följande gruppering 823 231 418 550 145 645 152. Dessa experiment har sedan kommit att bli en del av teorierna inom ämnet människa datorinteraktion och som en följd på hur gränssnittsdesign ska designas för att underlätta människors minnesförmåga (Preece et al, 2002). Baddeley et al (2004) beskriver långtidsminnet såsom bestående av två delar, explicit och implicit minne. Det explicita minnet kan i sin tur delas i sin tur in i ytterligare två delar; *episodisk* och *semantisk minne*. I det episodiska lagras minnet från exempelvis olyckor eller ens barndom, medan i det semantiska minnet är ord och betydelser som vi anser vara sanningar eller fakta. I det implicita minnet lagras den tacita kunskapen, alltså kunskap som vi inte kan uttrycka.

2.1.1 Varför glömmer vi?

Passer & Smith (2008) ger exempel på två olika teorier. Den första benämns *decay theory* och den andra *interference theory*. Decay theory kan enligt Passer & Smith (2008) förklaras enligt följande:

> *”decay theory, which proposed that with time and disuse the long-term physical memory trace in the nervous system fades away” (Passer & Smith, 2008, s.273)*

Passer & Smith (2008) hävdar att vi glömmer av flera olika orsaker. Glömskan kan uppstå i de tre olika faserna transformeringen, lagringen och framtagningen av informationen. De menar att det största minnesbortfallet sker vid transformeringen. Detta beror på att vi bara lagrar det vi är intresserade av och tenderar att filtrera information som är onödig. De hävdar även följande: *”Much of what we sense simply is not processed deeply enough to commit to memory” (*Passer & Smith, 2008 s.273). Av detta kan man dra slutsatsen att självklara saker, som inte kräver någon större bearbetning av hjärnan oftast leder till att vi glömmer det.

Den andra teorin, interference theory, består av två delteorier, vilka kallas för *proactive interference* och *retroactive interference*, båda fungerar i princip på samma sätt fast de är varandras motsatser. Proacative interference inträffar då vi lär oss nya saker som ska ersätta gamla och retroactive interference inträffar precis tvärtom, när vi lärt oss nya saker och som ska försöka minnas det gamla. Om en person blir tillfrågad vad ens nya telefonnummer är tenderar vi att enbart minnas en del av det eller enbart det gamla telefonnumret. Två månader senare är det dock inte säkert att personen minns det gamla numret. Det har ersatts av det nya telefonnumret vilket är en form av retroactive interference (Passer & Smith, 2008).

2.2 IT-säkerhet

Mitrović (2005) skriver att en normal verksamhet idag kan ha mellan 25 till 100 olika informationsdatabaser där användaridentiteter hanteras. Detta får till följd att arbetet med att hålla ordning på vilka användare, som har tillgång till vad blir mycket omfattande och krävande för de som administrerar systemet. Om databaserna inte kontinuerligt gallras på användare, riskerar antalet ”döda” användare att kunna utnyttjas av utomstående personer eller av tidigare anställda som av någon anledning hyser agg mot företaget eller organisationen, även kallat det interna hotet.

Mitrović (2005) påpekar att ett antal kriterier bör gälla vid skapande av lösenord och att *”En dålig hantering av lösenord är nästan inga lösenord alls”* (Mitrović, 2005 s.150)

- Välja ett bra lösenord
- Skydda sitt lösenord
- Ändra lösenordet på en periodisk basis
- Inte bygga på mönster

Han påpekar även att de viktigaste kriterierna för lösenord är att det är minst sju tecken långt och består av både siffror, bokstäver och specialtecken. För att påvisa skillnaderna av olika lösenords antal möjliga kombinationer se nedanstående tabell.

Tabell 1 Antalet lösenord och antalet kombinationer (baserad på Mitrović, 2005, s.151)

Lösenord		**Antalet möjliga kombinationer**
Bokstäver med två tecken	Ba	676
Bokstäver med fyra tecken	Defg	456 976
Bokstäver med sju tecken	Hijklmn	8 miljarder
Bokstäver och nummer på sju tecken	B1a2d3e	78 miljarder
Bokstäver, nummer och symboler på sex tecken	B2Cd£%	98 miljarder
Bokstäver, nummer och symboler på sju tecken	B2D3@$c	6 700 miljarder

2.3 Motivation

Magoulas & Pessi (1998) skriver i boken *Strategisk IT-management* att den infologiska ekvationen, *I=i(D,S,t)* , även kan omfatta motivation, M, och regler, R (Tabell 2).

Tabell 2 Beskriver den motivationsbaserade och regelbaserade infologiska ekvationen (baserad på Magoulas & Pessi, 1998, s.345)

regelbaserade infologiska ekvationen	**I = i((D +Dextra, S, t+textra),R)**
motivationsbaserade infologiska ekvationen	I = i((D +Dextra, S, t+textra),M)
Dextra	Externa faktorer eller ”extra data”
Textra	textra den extra tiden för tolkning

Magoulas & Pessi (1998) menar att vi människor styrs av belönings- och bestraffningssystem, vilket kan förklaras med att om vi människor blir bestraffade för att exempelvis inte ha lämnat in deklarationen eller inte betalat in skatten i tid så har vi grund för att ta till oss det åtagandet. Vi blir helt enkelt motiverade att genomföra uppgiften.

Motivation är en psykologiskprocess och kan enligt Nationalencyklopedin definieras enligt följande:

> *”Teorier om motivation förklarar varför vi över huvud taget handlar och varför vi gör vissa saker snarare än andra. De behövs för att vi skall förstå det faktum att organismer konsekvent strävar mot bestämda mål med hjälp av flexibla beteenden. Motivationskällan kan antingen förläggas inom personen eller organismen, som i instinkts eller drivkraftsteorier, eller i yttervärlden, som i s.k. incentivteori.”* (Öhman, 2008 (Ne.se))

Det är dessa olika behov som styr motivation och som i viss mån spelar in när vi transformerar syn och hörselintryck till data (D) och sedan lägger värde i det i form av de förkunskaperna (S). Magoulas & Pessi (1998) motivationsbaserade infologiska ekvation ger att om bristen av motivation när vi tar till oss data kommer vår möjlighet, alltså om M => 0 blir det allt svårare att ta till sig informationen.

2.3.1 Sammanfattning av motivation

När det gäller lösenord, och nyttan med lösenord är det rimligt att anta att lösenord delvis ses som problematiskt och jobbigt. Lösenord bör bestå av symboler och siffror och dessutom bytas periodvis (Mitrović, 2005). Det kan innebära att det är svårt att se någon logisk koppling i lösenord eftersom de inte skall följa samma mönster eller struktur, exempelvis A1B2C3XY och B2C2C4YZ. Detta leder många gånger till besvärligheter att tolka lösenord som information, då ekvationen påverkas av motivation. Vi kan även utifrån Mogoulas & Pessis (1998) regelbaserade infologiska ekvation och få fram att om det saknas motiv att lära sig lösenord tenderar användaren att handla så rationellt som möjligt. Om en användare inte

blir tillrättavisad att inte skriva lösenordet vid datorn eller på skrivbordet, leder detta till att användaren handlar rationellt och försöker göra det enkla i situationen, antingen genom att skriva ner lösenordet eller återanvända enkla lösenord för att inte glömma dem. Psykologerna Narine & Neath (1995) menar att människor kan ha svårt att minas ord som inte går att uttala. Enligt följande citat *"Memory is worse for items that take longer to pronounce, even when the items are equated for frequency, number of syllables, and number of phonemes"* (Narine & Neath, 1995, s.429).

2.4 Offentlig sektor

Det som vi i Sverige menar med offentlig sektorn, kan enligt SCB (2007) delas upp i tre delar; *den statliga sektorn, den kommunala sektorn* och *ålderspensionssystemet.* SCB skriver även att:

> *"Den offentliga sektorn är ett något vidare begrepp än offentliga myndigheter och omfattar offentligt ägda enheter som är "icke-marknadsproducenter", medan de offentliga myndigheterna endast omfattar den del av verksamheten som är skattefinansierad"* (SCB, 2007, s.25)

Den offentliga sektorn styrs också i högre grad av lagar och förordningar som antingen *skall* eller *får* genomföras. Den offentliga sektorn är indelad i olika ansvarsområden. Kommuner ansvarar för utbildning, plan- och byggfrågor, vatten och avlopp, räddningstjänst etc. Landsting och regioner ansvar för hälso- och sjukvård, kollektiv trafik, regional utveckling m.m. Staten ansvarar för lagstiftning, utrikespolitik, försvar, rättväsende etc.(SCB, 2007)

Både den offentliga och den privata sektorn styrs av mål. Målen skiljer sig åt, då målen inom offentlig sektor kännetecknas av att vara politiska och kontinuerliga (Jacbosen & Thorsvik, 2002). Företag drivs ofta av privata mål, vilka kan styras antingen av organisationer eller enskilda invidiver. De privatas mål kännetecknas av vinstintresse och konkreta mål som ”vi ska växa med 10 procent” istället för offentliga verksamheter som ”vi ska ge den bästa vården eller utbildningen”. Offentliga verksamheter erbjuder ofta tjänster som är komplicerade såsom missbruksvård eller undervisning. Jacobsen och Thorsvik (2002) skriver att *"offentliga organisationer ska drivas kostnadseffektivt"* (s.62). Detta står dock i strid med att offentliga verksamheter måste behandla alla grupper lika, allt ifrån skola till äldrevård. Detta styrks också i kommunallagen *"Kommuner och landsting skall behandla sina medlemmar lika, om det inte finns sakliga skäl för något annat."* (Kommunallag (1991:900 2kap 2§)). Då offentlig sektor inte kan agera fritt, utan är tvingad att tillhandahålla tjänster kan det innebära att medborgarna hamnar i en monopolsituation där medborgaren inte har någon annan aktör att välja mellan.

2.5 Single Sign-On

I detta avsnitt har vi delat in SSO i tre delar, i första delen definierar vi vad *Single Sign-On* är och hur det fungerar. I andra delen beskrivs *OpenID* som är en gratis SSO-tjänst där användare kan logga in på hemsidor som stödjer OpenID. Den tredje delen och sista delen beskriver vi *E-legitimation* som bl.a. banker använder sig av för att säkerställa identiteten för den som använder sig av avancerade Internettjänster.

2.5.1 Single Sign-On

SSO är en teknik, som gör det möjligt att komma åt flera system med en enda inloggning istället för att logga in enskilt på varje system. Det är först på senare tid SSO har slagit igenom, tidigare var det inte så stort problem då användare vanligtvis inte hade tillgång till så många system. Samar (1999) skriver följande:

> *"Now with the integration of web-based desktops and applications, the number of services a typical user accesses has grown multi-fold. It is no longer acceptable to enter one's username and password 25 times daily."* (Samar, 1999, s.1)

Acceptansen bland användarna har alltså minskat i takt med att det blir fler och fler inloggningar. Många har insett att i längden blir detta ohållbart och därför måste det till en förändring. Nedanstående citat definierar SSO enligt följande:

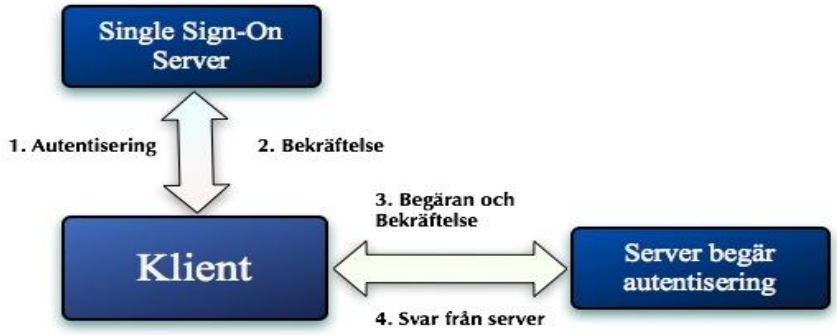
> *"Single Sign-On is a mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where that user has access permission, without the need to enter multiple passwords"* (Open Group, 2001).

> *"Single sign-on is a technique created to reduce the amount of authentications needed in a system to a minimum. A single sign-on system handles the authentication for services without user interaction"* (Falkcrona, 2008, s.8).

Tanken med SSO är att det ska underlätta för användaren genom att bara en inloggning krävs för att komma in i flera system istället för att logga in en gång på varje. SSO finns både på Internet och i interna system. Det finns idag ett flertal olika SSO-tekniker eller SSO-tjänster på Internet och där ingår blanda annat OpenID och e-legitimation. SSO kan också bidra till ökad säkerhet och minskade kostnader. Skräckexemplen med "post-it-lappar" är idag en vanligt förekommande säkerhetsrisk, speciellt då många har dessa lappar uppsatta på sin skärm eller någonstans på skrivbordet. SSO kan också bidra till kostnadsbesparing då färre användare behöver ringa till helpdesk för att få hjälp med konto och lösenordsrelaterade ärenden. Detta leder i sin tur till att produktiviteten minskar tillföljd av att användarna tvingas ägna mer tid åt konto- och lösenordshantering (Samar, 1999).

Det vanligaste sättet att logga in med SSO är genom att använda ett användarnamn och lösenord. I vissa fall kan det vara aktuellt att ”säkra upp” inloggningen med ett Smartcard eller fingeravtryckläsare och på det viset få en säkrare inloggning. Detta kan vara aktuellt då det finns extra känslig information som behöver mer säkerhet.

SSO är inte en specifik teknik utan det finns ett antal olika metoder som användas för att skapa en SSO arkitektur. Det finns två metoder som är vanligare än andra. Den ena är en ”ticket” baserad metod som bl.a. används av Kerberos (Falkcrona, 2008). Kerberos är ett autentiseringsprotokoll som används för att kommunicera över ett osäkert nätverk genom att bevisa sin identitet på ett säkert vis. Den andra är en ”cookie” baserad metod som används på Internet och kommunicerar med hjälp av ett HTTP-protokoll (Falkcrona, 2008). HTTP är ett protokoll som används för att föra över information på Internet. Med hänsyn till vår fokus har vi valt att inte fördjupa oss i hur SSO fungerar tekniskt. För att illustrera hur SSO kan se ut har vi valt att utgå från en enkel beskrivning över en SSO-lösning med HTTP-cookie. Klienten autentiserar sig mot en SSO-server (1), servern ger en bekräftelse (2), begäran och bekräftelsen skickas till servern (3) och servern svarar (4) (Falkcrona, 2008, s.8)



Figur 2 - Klienten autentiserar sig mot en SSO-server (1), servern ger en bekräftelse (2), begäran och bekräftelsen skickas till servern (3) och servern svarar (4) (Baserad på Falkcrona, 2008, s.8).

2.5.2 OpenID

OpenID är en webbaserad SSO-tjänst, eftersom OpenID bygger på öppna standarder och det är en gratis tjänst som alla kan använda sig av. Det finns idag ungefär tiotusen webbsidor som stödjer OpenID (OpenID.net, 2008a). Grundidén med OpenID är att användarna själva ska bidra till att OpenID växer genom att implementera tjänsten på sin egen hemsida eller sprida vidare information om OpenID. OpenID är inte bara för enskilda användare utan kan även användas av företag. OpenID.net skriver följande på sin hemsida:

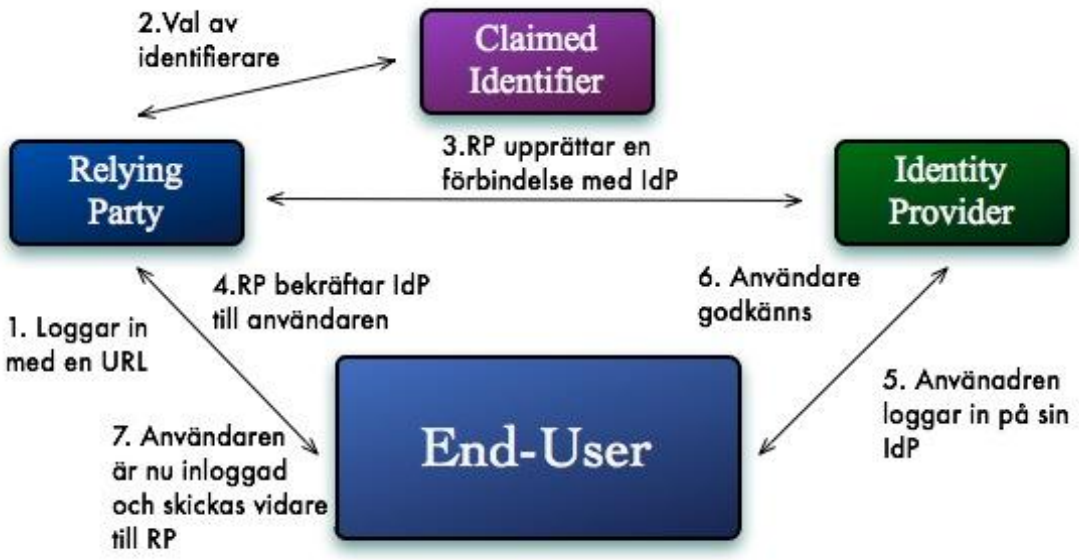
> *“For businesses, this means a lower cost of password and account management, while drawing new web traffic. OpenID lowers user frustration by letting users have control of their login*.”(OpenID.net, 2008a)

Enligt OpenID.net går det alltså att både spara in pengar vad gäller lösenordshantering och bidrar till att användarna känner att de har bättre kontroll över sina lösenord och användarkonton.

OpenID är uppbyggt så att alla användare måste registrera sig hos en OpenID Identity Provider (IdP) för att använda sig av OpenID. Det finns många redan etablerade tjänster som stödjer OpenID genom att vara IdP te.x. AOL, Blogger, Flickr, Yahoo och Wordpress (OpenID.net, 2008b). När användaren registrerat sig hos en IdP får användaren en URL/Adress som sedan används som inloggnings-ID på hemsidor som stödjer OpenID. De flesta sidor är alltså inte IdP utan stödjer bara OpenID inloggning. Så användaren behöver bara komma ihåg en URL och ett lösenord för att komma in på alla webbsidor som stödjer OpenID.

Tekniken som OpenID använder sig av för att identifiera en användare kallas ”Address-based identity” som bygger på att alla användare har en unik digital adress (Recorn och Reed, 2006,). En unik digital adress kan se ut på följande sätt ”openid.com/user” där Identity Providern är openid.com och user är det användarnamn som användaren är registrerad med. Istället för en URL går det också att använda sig av en XRI i-name som har samma funktion som en URL. Och kan se ut så här ”xri://=example.user” (Recorn och Reed, 2006).

OpenID autentisering bygger på att användaren ska bevisa att den ”äger” den URL:en som används vid inloggning. Detta görs genom att sidan som användaren vill logga in på även kallad ”Relying Party” och användarens OpenID Identity Provider (IdP) kommunicerar med varandra (Recordon & Reed, 2006). Användandet av URLs och XRIs som identifierare har den fördelen att ingen central autentisering behövs för användaren, Relying Parties eller Idintity Providers. Genom att använda sig av OpenID funktionen ”delegation” kan användaren behålla sitt publika OpenID identifierare även om den byter Identity Provider.



Figur 3 – Beskriver tillvägagångssättet vid användning av OpenID. (1) användaren loggar in, (2) användaren väljer identifierare, (3) identifieraren kontrolleras mot IdP, (4) RP bekräftar IdP för användaren, (5) användaren loggar in på IdP:n, (6) IdP:n godkänner användaren och användaren blir omdirigerad till RP (7) (Baserad på Recordon & Reeed, 2006 s.14)

2.5.3 E-legitimation

E-legitimation eller e-ID, som det också kallas, är en teknik för att kunna säkerställa sin identitet på nätet och kan ses som en form av SSO då man får tillgång till ett flertal tjänster oberoende av webbplats. Exempel på dessa tjänster är flyttanmälan, ansökan om studiemedel, personbevis, ändring av premiepensionsval etc. (CSN.se, Skatteverket, 2008). En del företag erbjuder idag också webbtjänster baserade på e-legitimation (E-legitimation.se, 2008a). Det finns idag fyra olika utfärdare av e-legitimation:

- BankID, en intresseorganisation som omfattar 9 olika banker (Bankid.com, 2008b)
- Nordea
- Telia
- Polisen eller VERVA (det nationella id-kortet)

En e-legitimation består antingen av en datafil eller av ett kort. Vid utfärdandet av en e-legitimation legitimerar sig användaren med hjälp av sin fysiska identifikation, antingen genom att logga in på sin Internetbank eller genom att beställa en kod från utfärden och hämta ut den genom att legitimera sig (e-legitimation.se, 2008b). Användandet av e-legitimationen bygger på att användare autentiserar e-legitimation med hjälp av ett lösenord. E-legitimation verifieras mot utfärdarens server och är e-legitimationen giltig godkänns användaren och så kan användaren logga in (Bankid.com, 2008a). Verket för verksamhetsutveckling, VERVA, utvärderar för närvarande på uppdrag av regering hur

framtidens e-legitimation ska utformas. Rapporten ska vara färdigställd i juni 2008. (Verva.se, 2008).

2.6 Metakatalog

Metakatalog är en typ av katalogtjänstteknik. Med katalogtjänst menas en hierarkisk ordnad databas innehållande olika objekt (Mitrović, 2005). Fördelen med hierarkiskt uppbyggda katalogtjänster är att de kan hantera många objekt samtidigt och de är lätta att administrera (Mitrović, 2005). Strukturen i en katalogtjänst kan jämföras med ett uppochner vänt träd där tilldelade rättigheters högts upp i träder ärvs av underliggande objekt. Som det ser ut idag är det vanligt att en organisation använder sig av flera olika katalogtjänster. Samverkan mellan dessa kan bidra till lägre administrationskostnader och säkrare behörighetsadministration (Mitrović, 2005). Metakatalog är en teknik som gör det möjligt för katalogtjänster att samverka. En metakatalogtjänst använder sig av tre metoder; *connectivity*, *brokeringsfunktionalitet* och *integritetsmekanismer* (Mitrović, 2005). Connectivity är till för att dela upp identitetsinformation mellan olika katalogtjänster. Med hjälp av borkeringsfunktionalitet kan förändringar gjorda i en katalog eller databas distribueras ut till de identitetslagringsplatser som är berörda av förändringen (Mitrović, 2005). Integritetsmekanismerna har till uppgift att se till så att synkroniseringen mellan identitetslagringsplatser fungerar korrekt.

3. Metod

I detta avsnitt beskriver vi hur vi gick tillväga och varför vi valde att använda oss av en kvalitativ forskningsmetod och vilka respondenterna var.

3.1 Metodval

Vi har gjort en studie i SSO inom offentlig sektor. Studien har en hermeneutisk prägel. Hermeneutisk betyder enligt Patel & Davidsson (2003); tolkningslära. Detta innebära att vi har analyserat, transkriberat och tolkat respondenternas svar. Inom naturvetenskapliga discipliner tillämpas motsatsen, positivistiskt synsätt. Detta innebär att man utgår ifrån verkliga samband och att forskningen inte påverkas av vare sig religiösa, tankar, siande eller analyser (Patel & Davidsson, 2003).

En uppsats kan antingen sägas vara deduktiv eller induktiv. Vi utgick inte ifrån en hypotes och studien kom därför att präglas av ett induktivt tillvägagångssätt, alltså att vi utarbetar en teori under studiens gång vilket innebär ”hypotesgenerande”. Motsatsen, deduktiv, kan ses som hypotesprövande, alltså att man vill tillämpa en tänkbar teori och bevisa om denna är sann. (Backman, 1998)

En forskningsmetod sägs kunna uttrycka sig antingen *kvantitativt* eller *kvalitativt*. En kvalitativ forskningsmetod utgår ifrån ”verbala formuleringar” (Backman, 1998). En kvantitativ metod innebär däremot att man utgår ifrån siffror och matematik och resulterar i statiskt data (Backman, 1998). Vi valde att använda oss av en kvalitativ forskningsmetod för att vi ville ta reda på de bakomliggande tankarna kring SSO. Vi ville komma åt respondenternas åsikter och detta är endast möjligt med en kvalitativ studie.

3.2 Urval

Vi har valt att inrikta oss på den kommunala sektorn på grund av dess heterogena ansvarsområde och begränsade tillgång på resurser.

Kontaktakten med kommunerna har skett i första hand via e-postmeddelande som sänds ut till kommunernas IT-chefer. Det vi efterfrågade var att komma i kontakt med två personer för intervju. Den första respondenten skulle bestå av en person som hade god kännedom av IT-systemmiljön och den andra skulle bisitta kunskap inom kommunens datorsupport (ofta benämnd helpdesk). Vi valde att rikta oss mot helpdeskpersonal för att bilda oss en uppfattning i hur vanligt det är med lösenordsrelaterade ärenden. Respondenterna med god kännedom om IT-verksamheten valdes ut för att vi skulle få en uppfattning kring deras tankar om SSO och säkerhet inom kommunerna.

Vi riktade in oss på kommuner i Göteborgsområdet utifrån geografiskt läge och personlig bakgrund, då en av författarna tidigare bott i en av kommunerna. Med hänsyn till personernas

integritet har vi anonymiserat personernas kön, ålder och kommuntillhörighet. Detta för att ingen skada ska kunna uppstå vare sig för den aktuella kommunen eller för den enskilde respondenten (Patel & Davidsson, 2003).

3.2.1 Beskrivning av kommunerna

Kommun A, större än 50 000 invånare

Kommun B, större än 50 000 invånare

Kommun C, mindre än 50 000 invånare

3.2.2 Beskrivning av intervjupersonerna

Datorsupport eller Help Desk

Respondent A, jobbar på Kommun A, har okänd utbildningsbakgrund.

Respondent B, jobbar på Kommun B, har okänd utbildningsbakgrund.

Respondent C, jobbar på Kommun C, har gymnasiebakgrund.

Ansvarig för IT-verksamheten

Respondent D, jobbar på Kommun A, har universitetsbakgrund.

Respondent E, jobbar på Kommun B, har universitetsbakgrund.

Respondent F, jobbar på Kommun C, har universitetsbakgrund.

3.3 Intervjufrågorna

Vid konstruktionen av frågorna utgick vi från boken *”Som man frågar får man svar”* (Andersson, 1985) och denna bok gav oss en fördjupad förståelse i intervjuteknik. De ämnen vi utgick ifrån när vi konstruerade frågorna var bland annat säkerhetsproblem, lösenordshantering och arbetsuppgifter. Ämnena bygger i sin tur på vad som framkom ur vår litteraturstudie. Utifrån dessa ämnen har vi utformat (se frågor Bilaga 1) fyra teman; *verksamhetssystem, lösenord, SSO* och *kontohantering*. Dessa har klassificerats utifrån de svar vi fått från respondenterna.

Anledning till varför vi använde oss av semistrukturerad intervjuteknik berodde på att vi inte ville ha en alltför ostrukturerad intervju, därför detta kan leda till en omfattande och tidskrävande analys. En ostrukturerad intervju ställer också högre krav på kunskaper och

erfarenheter i intervjuarteknik, vilken vi har begränsad erfarenhet av. (Patel & Davidsson, 2003). Preece et al (2002) hävdar dessutom att en alltför ostrukturerad intervju också kan bli i hög grad svåranalyserad och svår att jämföra med de andra intervjuerna.

3.4 Intervjuerna

Vårt mål innan studien var att genomföra sex till åtta intervjuer. Vi genomförde enbart fem, varav en skedde i grupp av två personer. Utöver dessa fem intervjuer genomförde vi även en uppföljningsintervju för att stämma av nyuppkommen fakta. I ett annat fall stämde vi av uppgifterna via e-post för att få ytterligare upplysningar. Intervjuerna varade mellan 25-50 minuter. De genomfördes i respondentens arbetsmiljö, antingen i ett konferensrum eller kontorsrum. Detta gjorde vi för att respondenten skulle känna sig trygg och att utfallet skulle bli det bästa för både oss och respondenten. Innan varje intervju tillfrågades respondenten om lov att spela in intervjun med hjälp av en mobiltelefon. Vi använde oss även av en digital diktafon som säkerhetskopia.

3.5 Analys av data

Direkt efter varje genomförd intervju hade vi en kort genomgång för att stämma av våra tankar och idéer om vad som framkommit. Utifrån genomgången bättrade vi på vår frågemall. Intervjuerna transkriberades i de flesta fall så fort som möjligt. När vi genomfört fem av de sex intervjuerna påbörjade vi arbetet med att sammanställa de transkriberade svaren i ett dokument. Därefter började vi gruppera svaren efter följande teman:

- *Verksamhetssystem*
- *Lösenord*
- *SSO*
- *Kontohantering*

4. Resultat och analys

I det här avsnittet ger vi resultatet av den empiriska studien med utgångspunkt av de nämnda temana; verksamhetssystem, lösenord, SSO och kontohantering

Ingen av kommunerna använder sig idag av SSO. Däremot är en av kommunerna i fas att införa det och har påbörjat ett projekt som ska leda fram till ett införande. Detta visar stöd för att ämnet är högaktuellt och vi kan fastslå att intresset även finns hos de övriga kommunerna, vilket även kommer visa sig i avsnittet Single Sign-On (4.3).

Vi kan konstatera att kommuner generellt fungerar på samma sätt men när det gäller IT-verksamheten är skillnaden mellan kommunerna påfallande. Vissa har valt att lägga ut verksamheten på entreprenad, andra har valt att behålla verksamheten inom kommunen. Av de olika kommuner vi intervjuade hade ingen lagt ut IT-verksamheten på entreprenad. Vi fick däremot kännedom om detta vid kontaktandet av kommunerna. En annan detalj som vi noterade var att det skilde sig organisatoriskt mellan kommunerna. Samtliga kommuner i vår studie hade valt att fördela supportansvaret av de olika förvaltningsspecifika systemen på respektive verksamhet. Däremot tillämpar kommunerna olika former av lösenordssupport vilket vi kommer gå in närmare på i avsnittet *Lösenord (4.2)*. Vi har valt att dela upp analysen i följande teman; *verksamhetssystem*, *lösenord*, *SSO* och *kontohantering*.

4.1 Verksamhetssystem

Kommuner är komplexa och omfattande organisationer. De har i uppgift att ansvara för en mängd olika servicetjänster som är till för medborgarna och som företag inte ser som marknadsekonomiskt lönsamma att ansvara för. Det handlar om alltifrån skola, vård och omsorg till skötsel av parker . Samtliga kommuner bekräftar bilden av att de har många system att administrera.

> *”Vi har nog 100-tal plus verksamhetssystem. Sedan har vi alla skolorna,* [de har] *ett par hundra system till.”*– **Respondent C**.

Respondent D och F uppskattar också att det rör sig om ett hundratal viktiga system som kommunerna använder sig av. Om man räknar alla bakomliggande system skulle antalet system bli ännu fler.

> *”Det är ju en 12 olika förvaltningar som har olika uppdrag så att sammanlagt har vi ju uppemot ett 100-tal viktiga system för olika verksamheter.”* – **Respondent D**

> *”... socialtjänsten både hemsjukvård och familjeomsorg, ekonomiskt bistånd, socialbidrag alltså det finns en hel uppsjö av system kring det då, och sen har vi alla tekniska förvaltningar. Husförvaltning har sina system, samhällsbyggnad har sina så sammantaget har vi ett 80*

> *tals system som man använder i verksamheten då. Då pratar jag inte om SQL-server då, det är mer bakomliggande system."* – **Respondent F**

Det är stor skillnad på hur många användare de olika systemen har. System som de flesta användare har tillgång till är Intranät, e-post och kalenderfunktion. Ekonomi, personaladministration och socialtjänstens system är de största verksamhetsspecifika systemen om man räknar till antalet användare. Med verksamhetsspecifika system menas system som är knutna till en viss verksamhet.

> *"... de [system] som är gemensamma för alla [är] alltså typ e-post och kalenderfunktion."*
> *"Men i mitten av allting så är ju personalsystem och ekonomisystem dem två viktigaste som hanterar våra två viktigaste resurser så att det är ju två tunga system"* – **Respondent D**

> *"... flest användare har ekonomisystemet alla som har budget ansvar går in och attesterar sina egna fakturor så det är ganska många. Personalsystemen vi har ju det där med självservice i det så alla anställda ska ju egentligen vara inne där. Socialtjänstens system är många naturligtvis. Intranätet, hemsidan är också många. Flest användare har vi nog i E-post systemet där har vi alla som är upplagda på något sätt med en dator. Största flest användare tänker jag då."*– **Respondent F**

En av anledningarna till att kommunerna har ansvar för så många system är att kommunernas verksamhet är mycket omfattande. Oftast är verksamheten specifikt inriktad på en viss domän så är dock inte fallet hos kommuner. **Respondent D** jämför en kommun med ett Sverige i miniatyr, vilket ger en väldigt bra återspegling på vad kommuner ägnar sig åt för verksamheter.

> *"Men det [kommunen] är ju ett Sverige i miniatyr kan man säga. Vi jobbar ju med alltifrån socialförvaltning med sina mer eller mindre hemliga system sekretessbelagda system till kulturförvaltning som vill skrika ut sitt budskap och alla använder ju IT-stöd på olika sätt men för helt olika syften. Där emellan finns ju alla andra förvaltningar som ja teknik, individ- och familjeomsorg."*– **Respondent D**

> *"I och med att vi är en kommun så har vi ju, om man bara inriktar sig på en sak har man ju bara de programmen man behöver, men här jobbar vi ju med allting."* – **Respondent C**

När det gäller administration av verksamhetssystem skiljer den sig åt mellan kommunerna. **Respondet E** och **F** beskriver hur de olika verksamheterna är organiserade. **Respondent E** framhäver att IT-enhetens ansvar sträcker sig till att hantera lösenord, medan supportrelaterade samtal om ett specifikt problem i ett verksamhetssystem inte är deras ansvarsområde. **Respondent F** däremot anser att teknikernas roll sträcker sig till att hantera tekniken och inte ge ut behörighet till höger och vänster. Respondenten anser även att det är nog med att teknikerna ansvarar för bakomliggande system. **Respondent A** är inne på att **Kommun A** tillämpar liknande förfarande som **Kommun C**.

> *”I alla övergripande större system hanterar vi lösenorderna, [vi] ansvarar däremot inte för själva verksamhetssystemet i sig så de kan inte ringa och fråga. ”Hur gör jag här?” inne i själva systemet. Då är det ute på förvaltningarna som man har ansvaret då, oftast kan de också byta lösenord i dom specifika systemen. Bara för att göra det enkelt för användarna så ska man kunna ett nummer som de ska kunna ringa oavsett vilket system dem behöver hjälper med då.” –* **Respondent E**

> *”[Vi] har rolluppdelat, det ska vara så det är inget fel utan tvärtom då blir rolleran väldigt tydligen, vem som gör vad. Teknikerna ska ju inte vara inne och lämna ut behörighet i personalsystem det är inte rätt. Det är illa nog att man kan hantera databasen. Det är teknik det handlar om och det är för tekniker, personalmänniska ska ju hantera informationen i systemen. Men det får ju vissa negativa effekter när det inte är uppkopplat på riktigt. Men taken är att det ska vara så.” –* **Respondent F**

> *”Det finns en massa förvaltningsspecifika applikationer som dem själva är ansvariga för som dem byter lösenord. Det kan jag inte ens göra. Vi guidar dem till vilken dem ska ringa då. Det är inte alltid så lätt för alla att veta. Allting som har med data har ju med oss att göra.”* **– Respondent A**

4.2 Lösenord

Vi kan konstatera att lösenordshantering är ett stort bekymmer ute i kommunerna, dock verkar de ansvariga för administrationen av lösenord inte inse att det är tidskrävande. Istället ser de oftast betydligt allvarligare säkerhetsaspekter i själva hanteringen av lösenord. En av respondenterna konstaterade dock att lösenord tar mycket tid i anspråk.

> *”... lösenordsbyte tar tid. Det är dem små bitarna som tar tid. Att hålla på med samma sak om och om igen. Det blir ju nog ett par timmar per vecka.”***– Respondent C**

Att hantering av lösenord är ett problem för alla kommunerna framkommer tydligt. En kommun sticker ut vad gäller antalet lösenordsrelaterade ärenden. Vi går in mer på varför i diskussionsavsnittet (5.2). Det är svårt att uppskatta hur många lösenordsrelaterade ärenden det är, eftersom vi inte har tagit del av någon statistik. Varje kommun har dock gjort en uppskattning om hur många ärenden de tror att det rör sig om.

> *”Uppskattningsvis mellan 5 och 10 per dag om vi smetar ut det på ett år.”* **– Respondent A**

> ”*Ett par gånger i timmen*” *”... ska man snitta ut det är så är det väl åtminstone en per timme.”***– Respondent C**

Om vi räknar med att en vanlig arbetsdag är på runt 8 timmar blir det 8-16 lösenordsrelaterade ärenden per dag. På frågan om det är mer än 20% lösenordsrelaterade ärenden svarar **Respondent E**:

> *”Det är absolut mer än 20%, det är kanske 50%?”*

Respondent B fyller i:

> *”Ja, det kan det väl vara 35% kanske.”*

Vi kan uppskatta att lösenordsrelaterade ärenden för **Kommun B** ligger någonstans mellan 35 - 50%. Detta kommer vi diskutera djupare i avsnitt Diskussion (5.2).

4.2.1 Lösenordsrelaterade ärendens variation över året

Det är också värt att konstatera att helger och semestrar verkar spela in i hur många som ringer angående lösenordsrelaterade ärenden. Det finns alltså ett antal yttre faktorer som kan påverka hur många lösenordsrelaterade ärenden det kan vara under en viss period. **Respondent C** pekar på att anställda glömmer av lösenord när de inte använt lösenordet under en lite längre tid än vanligt. **Respondent A** är mer inne på att anställda skjuter upp att ta kontakt med Help-Desk till ett senare tillfälle som passar bättre för den anställde.

> *”... måndagar är alltid värst… Ta en sådan sak som att nu är det klämdag på fredag, på måndag finns det inte en människa som kommer ihåg sitt lösenord. De klarar helgen, liksom är det fyra dagar så är det bortblåst"*– **Respondent C**

> *”Är det dåligt väder är det mer att göra till exempel är det semestrar som regnar då är det mer folk än när det är fint vänder. Det alltid mindre för helpdesk att göra före en långhelg folk bryr sig inte om att ringa förrän efter… efter helgen så ringer dem. Men man märker en nedgång innan semester och innan jul så börjar luta lite neråt. Dem svåraste problemen kommer alltid mellandagarna när det är personal som inte är van vid hantera saker.”***– Respondent A**

4.2.2 Hanteringen av lösenord

När det gäller hantering av lösenord kan man ställa sig frågande till hur de anställda hanterar sina lösenord. I många fall verkar inte kunskapen finnas om vad ett lösenord är till för utan man förvarar det fullt synligt på en lapp sittande på skärmen eller i närheten av datorn. På frågan:

”Vad är din uppfattning kring lösenordshanteringen?”

svarar **Respondent D:**

> *”Det är ju en disciplinfråga. Det är ju en upplysningsfråga i allra högsta grad och utbildningsfråga utav personal och sådant. Att man blir medveten om att det är en nyckel som man disponerar och att inte lånar ut sitt konto[till]sådana här saker.”*

Respondenten konstaterar att det finns ett problem och att upplysning samt utbildning av personalen skulle få de anställa mer medvetna om att det är en ”nyckel” som de ansvarar för.

Respondet C konstaterar att användarna tycker det är krångligt med lösenord men att de är bra på att komma ihåg sina pinkoder. **Respondent D** förstärker bilden av att lösenord är krångligt när den ger exempel på hur användarna kan missbruka sitt konto genom att låta en logga in och sedan låta alla använda kontot.

> *”Folk vet ju inte… De tycker det är krångligt med lösenord. Men de kommer inte ihåg det [lösenordet]. Men de kommer ihåg sina pinkoder och allting sådant men inte sina lösenord.”***– Respondent C**

> *”I vissa sammanhang är det ju så att man delar datorer alltså dom står så som någon gemensam resurs någonstans och det förekommer ju att någon loggar in och sen så får den datorn användas på det kontot.”***– Respondent D**

Både **Respondent A** och **C** är inne på problemet med att lösenord skrivs ner på lappar. **Respondent C** beskriver även ett problem med gruppkonton där de inte meddelar varandra att de bytt lösenord, vilket resulterar i många supportärenden.

> *”Socialtjänsten har ju många, många gruppboenden. Många gemensamma konton då.”*
> *”Så ringer någon och byter lösenord, nästa dag så ringer en annan som inte kommit in på hela natten. Jaha, då har de glömt sätta upp en lapp.”* **– Respondent C**

> *”Ja, men många har det på skärmen och sen så tittar man och ser [att de] strukit över en siffra och skrivit nästa. De har samma ord men de byter bara siffra på slutet.”***– Respondent A**

Respondent A menar att ur ett säkerhetsperspektiv kan det vara bättre att använda ett enklare lösenord som användare inte behöver skriva ner.

> *"... det [kan] vara bättre att en användare använder ett enkelt lösenord som dem själva kommer ihåg än att ha en lapp med ett svårt lösenord som de aldrig kan... Oftast säger man ju att man inte ska ha make, namn, barn som lösenord. Det är kanske bättre än att ha ~~*# uppklistrad som alla ser."*

I enstaka fall har det uppdagats rena säkerhetsöverträdelser då användare utnyttjat en f.d. anställds konto för olovlig Internetanvändning.

> *"Sedan finns det ju ställen där chefen samlat in alla lösenord så att det har hänt att det har varit ställen där det har varit 20 människor som använder samma lösenord för att logga in. Sedan kommer vi ut det är någon som har surfat på någon otillbörlig sida. Kan ni ta reda på vem det är? Ja, men den människan har inte jobbat här på tre år. Det är ett konto då som inte är avslutat. De har använt samma"* **– Respondent A**

4.2.3 Byte av lösenord och krav på lösenord

Kommunerna tillämpar lite olika rutiner när det gäller byte av lösenord. Två av kommunerna tillämpar periodvis byte av lösenord, medan den tredje kommunen tillämpar för närvarande tilldelade lösenord men planerar att införa periodvis byte.

> *"Nuvarande lösning är baserad på tilldelade lösenord. Minst 6 tecken. Mix av siffror och bokstäver, min 2 siffror, gemener och versaler blandas… det går att byta genom att bli tilldelad ett nytt lösenord."* **– Respondent D**

Respondent C säger att de för närvarande tillämpar följande lösenordspolicy.

> *"Idagens läge så är det 8 tecken, inga å ä ö, det är väl det vi brukar säga till dom. När vi sätter lösenord så trycker vi in lite siffror och grejer för dem."*

De har dock haft en diskussion om att höja säkerhetsnivån när det gäller kravet på vad lösenord ska uppfylla.

"När vi ska gå över till vårt nya nät så ska vi ju passera 3 av 4 kriterier, stora, små, siffror och specialtecken tre av dem måste uppfyllas vilket inte är aktivt än nu." **Respondent C** säger att kommunen i dagsläget tillämpar

> *"Om jag säger deras inloggningslösen så är det 100 dagar. Där vill vi ha lite till. Vissa har 200 dagar. Men standarden är 100 är det sagt."* **– Respondent C**

Respondent B och **E** menar att deras kommuns policy är att tillämpa periodvisbyte

> *”Ja man måste förnya det en gång i månaden och det ställer ju till det då för de kommer inte ihåg vad det har bytt till.” ”Kravet är också att lösenordet inte får växla mellan två lösenord.”*
> *” 12 eller 13 ... du kan inte ta något som du har haft tidigare … [och] du måste ha minst 8 tecken så att det kan vara lite olika i olika system men vårt nätverk är minst 8 tecken .. [sedan så] försöker vi att tala om för dom att det ska vara lite komplext med både bokstäver och siffror och inga å ä och ö.”*

De uppmanar användarna att istället för att skriva ner sina lösenord att enbart använda ett enda och byta detta på alla system.

> *”Vi försöker ju att tala om det för användare som har många lösenord att byta samtidigt och sätta samma lösenord. Då har man ju en chans att komma ihåg det faktiskt det är bättre än gula lappar under tangentbordet. Vi har ju en IT-säkerhetshandbok för användare där vi ger tips hur de ska hantera [det] här med lösenord... Ni kan gärna ta med er den”*

Respondent C ger en förklaring till varför å, ä och ö inte får förekomma i deras system och vi utgår ifrån att detsamma gäller i **Kommun B** ”*Det finns vissa system som inte registrerar å, ä, ö så om vi printar det i dem så kommer dom inte använda det.”*

4.3 Single Sign-On (SSO)

Det råder delade meningar bland respondenterna av nyttan med SSO och de konsekvenser det medför.

4.3.1 Inställningen till SSO

Respondent C ställer frågan till oss om SSO är säkert och konstaterar *”Men Single Sign-On [som] sådant så? Är inte det en säkerhetsrisk någonstans? Ett lösen kommer ut så kommer man åt allting?”* Detta bekräftar säkerhetsproblematik kring SSO och vilka konsekvenser det kan få om det lösenordet kommer ut.

Respondent D resonerar att SSO i teorin är god men i praktiken är svårt att genomföra, då det råder en omfattande heterogen systemmiljö och att varje system har sin användarhantering.

> *”Rent teoretiskt är det väldigt bra men det är väldigt svårt att genomföra. Vi har himla många olika system som vi jobbar med. Vi har ofta inbyggda inloggningssystem [och] användarhantering ligger ju inne i systemet och det kan många gånger vara svårt komma åt*

> *dem här lösningarna med någon form utav centrallösningar att jobba med AD[1] metakataloger och sådana saker för att."* **- Respondent D**

Respondent D anser trots det att SSO skulle underlätta en del, dock krävs det en hel del förändringar enligt **Respondent D**, om för att det ska fungera. Respondent D konstaterar även risken med ett lösenord och tillgång till alla system och relaterar till användarens hantering av lösenord.

> *"Skulle man lösa det här på ett bra sätt så finns det väl många fördelar men som sagt det finns ju risker med det också för om någon kan koden så att säga på ett konto så får man ju ganska vid tillgång till systemet. Det är väl baksidan med sådana här Single Sign-on. Tyvärr så står ju ibland inloggning och password under tangentbordet och sådana här saker. Det är ju alltid baksidan på sådana här standardiseringar. Hittar man nyckeln så är man inne i alla system."***– Respondent D**

Respondent F ser SSO i ett större sammanhang än inom den interna IT-verksamheten och delar upp det i interna, kommunal, regional och nationell nivå.

Intern nivå

Den interna är där kommunens system verksamhetsspecifika system ingår.

> *"Vi kommer ju hamna i det och vi behöver [ju] det naturligtvis men det finns inte det där riktiga drivet och förutsättningarna idag tycker jag."* **– Respondent F**

Respondent F delar **Respondent Ds** uppfattning om att användaradministrationen i system är ett problem men utvecklar det till att systemtillverkarna vill "äga" användarna. Detta visar en sida av de tekniska svårigheterna med att införa SSO.

> *"…men återigen alltså få våra verksamhetssystem att fungera med SSO de är det som det handlar om. Vi vill ha det men det är svårt att köpa det för pengar som vi har. Det är inte en standard funktion i systemet utan var och en vill äga sina användare om man är systemleverantörer då, alla vill vara mitten alla vill vara portalen internt."* **– Respondent F**

[1] *"Active Directory (AD) is an implementation of LDAP directory services by Microsoft for use primarily in Windows environments. Its main purpose is to provide central authentication and authorization services for Windows-based computers"* (Wikipedia, 2008).

Kommunal nivå

Med kommunal nivå syftar vi på kommunens åtagande gentemot medborgaren och såkallade elektroniska medborgartjänster.

Både **Respondent F** och **Respondent D** nämner e-ID som en form av identifiering vid användandet av såkallade medborgartjänster. **Respondent F** menar att kostnadsbilden i dagsläget är för hög vid användandet av e-legitimation för verifiering av medborgaren. Dessutom råder det oenighet kring vilken e-legitimationsstandard som ska användas. Detta förklaras mer utförligt i avsnitt Diskussion (5.).

> *”de systemen som finns idag är lite oförutsägbara för det är så många uppslag mot Bankid och Telias lösning eller vilken man väljer. De är inte anpassade för kommunalverksamhet om jag som förälder går in och kollar på min elev”*

> *”Det som är svårt att få grepp om idag är vem man förväntar sig ska göra vad så inte varje kommun tar fram ett certifikat, det borde vara en nationell angelägenhet.”* **– Respondent F**

> *”Dessutom ska kommunen betala för varje uppslag att jag är jag vad jag har tittat på. Vi måste få en flat rate tror jag, och då får vi en infrastruktur för SSO [på] nationell nivå kan man säga.”* **– Respondent F**

Regional och nationell nivå

Respondent F menar att ansvaret för införandet av e-ID ligger på regional och nationell nivå.

> *”Det här har diskuterats väldigt mycket i Göteborgsregionen bland kommunerna, det har diskuterat mycket på regions nivå och det har diskuterats mycket nationellt.”*

Men även **Respondent D** är inne på att användandet av e-ID är ett problem och att det förts diskussioner under lång tid.

> *”inte minst på medborgarsidan har det ju vart mycket diskussioner om det här med e-id men med tanke på att det inte finns någon gemensam standard så kommer det liksom inte loss.”*

Respondent E säger att de varit på gång länge med SSO men av olika anledningar har det inte blivit av.

> *”Vi har ju vart på gång i ett antal år egentligen vi har ju [ett] sådant metakatalogprojekt det är ändå det som ligger till grund för mycket av dom här delarna. Vi kommer sätta igång med detta nu nästa*

> *fredag. Vi har vart på gång problemet har vart att vi inte har resurser tillräckligt och lägga tiden."*

I och med detta svar fick vi därför anledningen att genomföra en uppföljningsintervju, dock kom det att visa sig att workshoppen de tänkt hålla blev uppskjuten på grund av sjukdom. De kommer därför att påbörja projektet efter denna studies avslutande.

Respondent E menar att de största orsakerna till varför de tänkt införa SSO är komplexiteten med användaradministrationen.

> *"Mycket handlar ju om användaradministration den är för komplex idag. Det ska läggas upp användare på massa olika ställen. När användare slutar så meddelas inte det på rätt sätt utan de ligger kvar så vi har fått hitta på egna lösningar för att de inte ska finnas kvar under allt för lång tid då."*

De är den enda av kommunerna som i studien tillämpar inaktivitet som spärrfunktion för att förhindra att obehöriga ska kunna utnyttja ett konto som står outnyttjat. Detta behandlas mer under avsnitt konto (4.4). Vid införandet av SSO har de **(Kommun B)** valt att utgå ifrån personalsystemet och ger följande förklaring:

> *"... där kommer man alltid in och där försvinner man alltid när man slutar, man har inte lön när man slutat så det är det systemet som vi har sagt ska vara det som styr allt annat."* **– Respondent E**

De nämner dock att de inte kommer tillåta access till alla system, utan kommer kräva en extra på loggning.

> *"Det kommer nog bli lite både och i vissa system kanske man kommer ha den lösningen att man kommer in med automatik i andra system kan det vara så att man har samma lösenord med måste logga på sig igen så att det finns lite olika tankar."***– Respondent E**

Detta förklaras med att om användaren loggar på sig och låter datorn stå och sen lämnar datorn då finns det en stor risk i att någon annan kan komma över informationen i det systemet.

På frågan om *"vilka konkreta vinster de ser med SSO?"* svarar **Kommun B** att det i slutändan handlar om besparing av tjänster.

> *"Ja, alltså ska man se kallt på det här så är det ju tjänster som det handlar om. I kommunen är det ju mesta det dels i sista änden. Vi kommer att istället fokusera [på att] effektivisera hantering och att man som administratör, som det nu man har ju redan tagit bort dem här assistent tjänsterna."*
>
> *"Det är våran organisation som kommer att minska, om det nu blir så effektivt som vi har tänkt oss."* **– Respondent E**

4.3.2 Inställningen till OpenID

Respondenterna anser att det inte är moget för kommunal verksamhet i dagsläget. **Respondent F** resonerar även vidare och undrar vem som ska vara ansvarig support av en sådan tjänst och relaterar detta till Linux. **Respondent D** och **F** delar uppfattningen att webbaserade system är på väg in i den verksamheten, men att det fortfarande klientbaserade lösningar som är vanligast.

> *”Jag har läst lite om det [och] jag har funderat är det moget? Jag känner inte till att det används så mycket i kommunala världen. Jag håller mig på den nivån kan man säga jag fördjupar mig inte mer i det just nu.”*– **Respondent F**

> *”Men det bygger ju på att tillämplingarna är webbaserade Internetbaserade tyvärr är det så att mycket utav det som vi jobbar med i kommunal är ju gamla tillämplingar. Klientbaserade så att. Det är ju också naturligtvis en strävan som vi har av olika att gå mot webbaserade verksamhetssystem”* **– Respondent D**

Det är anmärkningsvärt att till och med systemleverantör inte kan erbjuda webbaseradesystem utan ser enbart nyttan med klientbaseradesystem. Respondent D konstaterar att samarbetet mellan kommunerna borde fungera bättre i detta sammanhang.

> *”För min egen del tycker jag det är skrämmande att leverantörerna kan uppföra sig på det viset. Jag menar att det är vi kommuner som är dåliga på [att] samordna oss och sätta tryck på marknaden men så fungerar det. Så det har ingenting med ålder hur länge vi har använt systemen.* **– Respondent D**

4.4 Kontohantering

Vi ville även undersöka vilka rutiner det finns vid en användares händelseförlopp, alltså från att ett användarkonto skapas tills att användarkontot avslutas på grund av avslutad anställning. Man kan konstatera att rutinerna i skapande av användarkontot inte skiljer sig nämnvärt åt mellan de olika kommunerna. Vi har valt att dela in konto i tre undergrupper när *konto skapas*, *utfärdande av nytt lösenord* och *konto avslutas*.

4.4.1 Konto skapas

När en anställd ska börja och få ett konto skiljer sig förfarandet mellan kommunerna inte nämnvärt.

> *”Då får vi in en lapp eller digitalt alla användaruppgifter som vi behöver vad dem heter när dem är födda och så här så skapar vi ett standardlösenord och tvingar dem att byta vid första inloggningen”*

– Respondent C

En anställd får oftast till en början tillgång till de vanligaste systemen e-post, Intranät etc. Tillgången till verksamhetsspecifika system utökas successivt beroende på vilken befattning den anställde innehar.

4.4.2 Utfärdandet av nytt lösenord

Med hänsyn till att lösenord är av känslig natur har vi av säkerhetsskäl i detta avsnitt inte relaterat ett citat till en respondet eller kommun. Av nedanstående svar kan vi konstatera att lösenordsrutinerna skiljer sig åt mellan kommunerna. En kommun utmärker sig överlag i säkerhets tänket.

”De ringer in hit och så säger de inte kan logga in i system X till exempel, oavsett vad det är för lösenord så har vi alltid en motfråga, vem dom är, vad dom sitter någonstans, personnummer och sen är det också en motringning som görs då på telefonnummer så att den personen faktiskt sitter där den ska sitta.”

En annan kommun ger följande bild av hur lösenordstilldelningen går till och ger inte lika förtroendeingivande svar.

”Det finns ingen kontroll. När man väl knäckt standarden vi har ju användarnamn baserat på vad de heter. En gammal version. Det blir många användare.”

Den tredje kommunen ger sin bild av lösenordstilldelningen och anser att kontrollen av lösenord är omöjlig att göra via telefon, dock tillämpar de kontroll av personnummer.

”Vi frågar ju alltid efter personnummer. Grejen är ju att man kan höra på människor när det rabblar sitt personnummer”

4.4.3 Kontot avslutas

Det kanske mest intressanta för vår del är hur rutinerna fungerar när en anställd slutar. Vi kan konstatera att alla kommuner har problem med såkallade ”döda” konton. Ett dött konto är när en användare slutat och detta inte blivit bortaget. Det döda kontot kan då komma att utnyttjas för intrång eller användas av andra anställda för ej avsedda uppgifter till exempel att surfa på arbetstid.

”När dom slutar så deletar vi rubbet. Vissa som går pension och vissa som är sommarjobbare kan man då sätta inaktivt. De som går i pension 2 månader senare så är dom tillbaka. För då har det inte blivit ett vettigt överlämnande så är dem här ett halvår till och tjänar

> *pengar. När dom går i pension så är det oftast bara [att] inaktivera dom"* – **Respondent C**

Kommun B tillämpar en form av inaktivering för att deras rutiner kring att anmäla att anställda inte slutar.

> *" efter tre månader så blir du spärrad då problemet med det då kan ju vara att det finns personer som är tjänstlediga och mammalediga osv. Dom kommer också bli spärrade med det är ett sätt för oss i alla fall att undvika att det ligger kvar i vårt system i flera år, så att det är den rutinen vi har idag då. Så är det så att någon kommer tillbaka kan man plocka tillbaka någon."* **– Respondent E**

> *"Två månader är det"* rättar **Respondent B**

I **Kommun C** tillämpar de inte inaktivering och Respondent C konstaterar att det förmodligen kan finnas konton kvar som inte används. När Respondent C inser detta funderar den hur detta kan kollas.

> *"Det ligger nog ett par konton som inte används. Jag vet inte om det finns något sätt att kolla på det. De går ju inte och lägger sig som inaktiva. Då får man ju kolla senaste loggin datum då. Skoj. Det har jag faktiskt inte tänkt på"* – **Respondent C**

Kommun A tillämpar rutinen att det ska komma in ett papper underskrivet av chefen.

> *"Den är man ju lite försiktig, därför det kan ju finnas någonting som i kontot de skulle ha så det går ju bara med några få knapptryckningar förstöra ganska mycket grejer så man brukar hålla på det en stund så det verkligen har tömt sina mappar och grejer. Vi brukar ju spärra det från den dagen, men det finns ju kvar det går ju att öppna igen."*- **Respondent A**

Samtliga kommuner applicerar försöksinloggningsrutin, alltså att ett konto blir spärrat efter ett visst antal försök. Detta varierar mellan tre till fem beroende på kommun. Både **Respondent D** och **Respondent F** konstaterar att det är ett problem med döda konton. **Respondent D** menar dock att de är i fas att införa en metakatalog.

> *"Det är alltid ett problem men där håller vi på att införa kontohanteringssystem som ska hämta signaler som ifrån personalsystemet, lön slutar att betalas så ska det utlösa en kaskad händelse. Kataloger i karantän stänga kontot stänga telefon och sådana saker. Det är ett arbete som är igång uppe på driftsidan så att. "* – **Respondent D**

Respondent F tvingas motvilligt erkänna att det finns gamla konton som inte används.

”Det ska ju inte göra det, det är klart det inte görs eller det är klart det gör. Vissa system är sämre än andra så är det. Framförallt är det inte säkert att man har samma användaridentitet i olika system, inte så självklart att koppla ihop de när de väl har metakatalog t.ex.”

5. Diskussion

I det här avsnittet diskuterar vi resultatet som framkommit och gör bland annat återkoppling till vårt teoretiska ramverk som vi utgått ifrån. Vi diskuterar med utgångspunkt från våra teman: Verksamhetssystem, Lösenord, SSO och Kontohantering.

5.1 Verksamhetssystem

Utifrån resultatet kan vi konstatera att kommuner har en vidd systemmiljö, vilket således bekräftar vår uppfattning att kommuner förfogar över många system. Med utgångspunkt från vår teoretiska del om offentlig sektor, bekräftas bilden om att kommuner ansvarar för en mängd olika verksamheter (SCB, 2007). En av respondenternas konstaterande *"[kommunen] är ju ett Sverige i miniatyr kan man säga."*, styrker vårt antagande.

Vi kan konstatera att kommunerna har många system, dock är det ett fåtal av dessa som används i större omfattning. De system som i princip alla användare har tillgång till är e-post, Intranät och hemsida. Vanligtvis har en användare även möjlighet att utnyttja ett eller flera verksamhetsspecifika system exempelvis personaladministration (självservice), ekonomi och socialtjänstens olika system.

Vi har identifierat att kommunerna antingen använder sig av centraliserad eller decentraliserad lösenordshantering för sina verksamhetssystem. Kommun B tillämpar centraliserad lösenordshantering vilket medför att användarna i de flesta fall enbart behöver ringa ett samtal till supporten för att få ut sitt lösenord till det verksamhetsspecifika systemet. **Kommun A** och **C**:s helpdesk ansvarar enbart lösenordstilldelning för inloggning på datorn och e-post. Detta ser vi som en form av decentraliserad lösenordsadministration.

5.2 Lösenord

Det råder en hög osäkerhetsfaktor i frågan om hur många lösenordsrelaterade ärenden som kommunerna hanterar och utifrån detta inte valt göra någon uppskattning. Respondenterna bekräftar dock vårt antagande av att lösenordsrelaterade ärenden är frekvent förekommande, men de understryker hellre hantering av lösenord som ett värre säkerhetsproblem.

Variationen av lösenordsrelaterad problemet kan relateras till decay theory (Passer & Smith, 2008) som grundar sig i att människans tenderar till att glömma efter en längre tid.

När det avser hantering av lösenord blir vi förvånade över respondenternas svar att användarna förvarar sina lösenord i närheten av datorn. Detta tyder på avsaknaden av rutiner för fysisk säkerhet. De bakomliggande faktorer kan vara många, dock tenderar detta att främst bero på organisatoriska brister. Vad vi dock kan konstatera av antalet lösenordsrelaterade ärenden är att det överrespresenteras i **Kommun B**. Detta har sin grund i att de tillämpar centraliserad lösenordstilldelning och tillhandahåller nästintill alla lösenord.

Tillvägagångssättet för att få ut ett lösenord för ett verksamhetsspecifikt system i en decentraliserad lösenordsorganisation, kräver däremot att användaren vänder sig till respektive systemägare eller systemförvaltare. Detta innebär ofta att användaren i första hand vänder sig till supporten och får då reda på att han eller hon ska kontakta sin systemadministratör. Eftersom inte supporten ansvarar för detta riskerar det att bli omständigt för användaren om systemägaren inte är tillgänglig. Samtidigt finns det ett säkerhetstänkande som en av respondenterna betonar vikten av i rollbaserad ansvarsfördelning. ”*Teknikerna ska ju inte vara inne och lämna ut behörighet i personalsystem det är inte rätt. Det är illa nog att man kan hantera databasen.”* Vi ifrågasätter rolluppdelandet då respondenten reflekterar över teknikernas roll och samtidigt konstaterar att teknikerna har ansvar för de bakomliggande systemen, dock delar vi åsikten om att det är svårt att säkerställa identifiering av användare i en omfattande verksamhet. Vi har inte undersökt systemförvaltarens eller systemägarens arbetsuppgifter och kan därför inte uttalas oss. Däremot har vi fått uppfattning om att de innehar en ordinarie tjänst. Om detta stämmer kan det innebära att ett lösenordsrelaterat ärende dröjer avsevärt längre tid än om helpdesken hade löst ärendet.

Användaren har oftast lättare att komma ihåg lösenord som består av saker de känner igen eller känner relation till än hävdar en respondenterna *”Oftast säger man ju att man inte ska ha make, namn, barn som lösenord. Det är kanske bättre än att ha ~~*# uppklistrad som alla ser.”* Detta kan kopplas till vårt teoriska ramverk om att det är enklare uttala ett ord eller en mening än ett ord bestående av siffror, bokstäver, specialtecken (Nearine & Neath, 1995).

När det gäller lösenordsbyten varierar det emellan kommunerna, dock utmärker sig Kommun B då de tillämpar lösenordsbyte varje månad. I motsatsen utmärker sig Kommun A då de för närvarande inte tillämpar lösenordsbyte. Lösenordsbyten kan relateras till interferens teorin som grundas på att människan har svårt att komma ihåg sitt gamla lösenord (Passer & Smith, 2008).

5.3 Single Sign-On

En kedja är inte starkare än den svagaste länken och i fallet säkerhet är detta avgörande. Det spelar ingen roll att man har lösenord om människor ändå handlar omdömeslöst. Att lösenord skrivs på skärmen eller under tangentbordet kommer ändå innebära problem, då förloras funktionen och tankarna med säkerheten och SSO. SSO innebär att ett enda lösenord används och åsikterna är delade kring riskerna. En del anser att SSO innebär en säkerhetsrisk, då det helt enkelt används ett enda lösenord och vips är man inne i alla system, andra ser helt enkelt inte baksidan med att det redan existerar en ”falsk” SSO framförallt då användare tenderar använda samma lösenord i flera system. En av de intervjuade kommunerna uppmanar till och med att byta samtliga för att minska bördan för supporten. Självfallet innebär SSO en säkerhetsrisk om SSO-lösenordet kommer på avvägar. Dessutom krävs det högre säkerhet på SSO-lösenordet. Idag tillämpar ingen av de kommuner vi talat med den säkerhet som anses vedertagen på lösenord, det vill säga minst sju tecken, som består av en blandning av siffror,

gemener, versaler och symboler (Mitrović, 2005), dock har en kommun planer på att införa högre säkerhet. Kommun A tillämpar tilldelade lösenord vilket gissningsvis innebär högre säkerhet, dock minst sex till tecken vilket å andra sidan blir mer osäkert (Mitrović, 2005).

Respondenterna ger en bild av att SSO är en teknologi som de tror på, dock så använder inte någon av kommunerna SSO i dagsläget. En av kommunerna är emellertid i fas att påbörja ett projekt som kommer leda fram till en SSO-lösning. De andra kommunerna ligger steget efter men har eller är i fas att införa en metakatalogstruktur.

5.3.1 e-ID

Oklarheten i e-ID eller e-legitimation grundar sig på att det för närvarande inte finns en gemensam standard, utan istället är det tre olika standarder. Verket för verksamhetsförvaltning, VERVA, utreder, på uppdrag av regeringen, för närvarande hur framtidens e-legitimation ska se ut (Verva.se). Respondenterna påpekar detta i sina svar och anser att det är ett hinder för att införa såkallade medborgartjänster. Detta delas av Sveriges-Kommuner och Landsting, SKL, som förordar att ”*staten ska utfärda, garantera och finansiera en nationell elektronisk identitet för fysiska och juridiska personer”*, teknisk och fysisk plattformsoberoende (mobil, smarta kort, dator etc.) samt bygga på öppna och hållbara standarder (SKL.se, 2008)

Respondenternas svar kan även härledas till Statskontorets (1999) såkallade 24-timmarsmyndighetsvision. Den definierar 24-timmarsmyndigheten i en utvecklingstrappa bestående av fyra kriterier. De tre första kriterierna berör hur information ska presenteras och förmedlas på webbplatsen. Det fjärde och sista kriteriet definieras enligt följande *”Webbplats och nätverksfunktioner för samverkan med andra myndigheter och samhälleliga instanser.”* (Statskontoret, 2000:21 s.8). 24-timmarsmyndighetskriterina ska dock enbart ses som ett kontinuerligt mål och är svårutvärderat. Antalet offentliga verksamheter som uppfyllt sista kriteriet är dock få. Då det här kravet innebär samverkan mellan offentliga verksamheter. Dessa avancerade tjänster mellan organisationerna kräver i sin tur säkerställande av identiteten.

5.3.2 OpenID

Intresset för OpenID är i dagsläget svalt och det har sin förklaring i att det saknas infrastruktur för att det ska vara intressant. OpenID bygger på webbteknik och för närvarande är kommunernas system oftast klientbaserade.

5.4 Kontohantering

Vi kan konstatera att kontohanteringen skiljer sig åt i rutinerna för att få ut sitt lösenord mellan kommunerna. En av kommunerna tillämpar högre säkerhet vid utgivandet av lösenord, dock kan vi inte utveckla detta då vi kan röja anonymiteten för vissa respondenter eller kommuner. När det gäller rutinerna i avslutandet av konton skiljer detta sig åt. Ingen av

kommunerna kan garantera att det inte förekommer döda konton, emellertid har en av kommunerna valt att utveckla en inaktiveringsfunktion för att förhindra att kontot finns tillgängligt under längre tidsperioder av inaktivitet. I ett fall fick vi det bekräftat av respondenten att kontot har utnyttjats av anställda för olovligt ändamål.

6. Slutsats

I det här avsnittet görs en slutsats av studien och det vi kommit fram till utifrån vårt resultat- och diskussionsavsnitt.

Lösenordshantering är ett svårhanterligt problem och det skiljer sig åt mellan hur kommunerna valt att organisera detta. Vi har identifierat två olika tillväggångssätt; *centraliserad* eller *decentraliserad* lösenordshantering. I vår studie har vi inte undersökt vilket av tillvägagångssätten som är säkrast, men vi anser oss trots detta vara övertygade om att en centraliserad lösenordshantering bidrar till en bättre överblick. Detta resulterar i att kommunen ser hur omfattande problematiken med lösenordshanteringen är och får verksamheten att överväga över införandet av SSO.

Vi vill återkoppla till de frågor som vi ställde i inledningen, som var vår utgångspunkt för denna studie:
Vilka faktorer får en offentlig verksamhet att införa Single Sign-On?
Innebär Single Sign-On en ekonomisk nytta?
Vilka säkerhetsaspekter finns det i att använda Single Sign-On i affärskritiskverksamhet?
Hur kan en offentlig verksamhet tillgodose sig nyttan av OpenID?

Och avslutningsvis vår huvudfråga: *Vilka aspekter bör beaktas vid användandet av Single Sign-On inom offentlig sektor?*

6.1 Vilka faktorer får en offentlig verksamhet att införa SSO?

Det finns flera faktorer som får en offentlig verksamhet att inför SSO. Vi har identifierat följande tre faktorer.

- *Helhetsperspektiv* – För att förstå komplexiteten med lösenordshantering måste man först skaffa sig en överblick av användarhantering och lösenordshantering.
- *Säkerhet* – Minskar risken med ”döda” konton och minskar risken att användaren försummar lösenorden.
- *Ekonomiska* **–** Leder till effektivitet och kan i slutändan leda till färre tjänster.

6.2 Innebär Single Sign-On en ekonomisk nytta?

Då enbart en kommun tagit ställning till att införa SSO och vi inte kunnat få fram någon ekonomisk kalkyl eller budget, anser vi frågan är svårbesvarad. Däremot är kostnaden för användaradministrationen betydande, då en administratör tvingas lägga upp ett konto i varje system och samma förfarande gäller vid bortagande av konto. Innebär SSO dessutom en tidsvinst för den anställde i en verksamhet med många system och åtskilda användarnamn (Samar, 1999). För en decentraliserad användarhantering innebär ett införande av SSO en

betydande vinst, då användaren kan tvingas söka upp systemägaren och om denne inte är på plats går dyrbar arbetstid förlorad.

6.3 Vilka säkerhetsaspekter finns det i att använda Single Sign-On i affärskritiskverksamhet?

Frågan kan delas upp i två svar beroende på hur man definierar affärskritiskverksamhet. Om vi utgår från de system som används av flest användare, alltså e-post, intranät, Internet eller kalender kan vi inte identifiera några direkta risker. Däremot om vi inkluderar verksamhetsspecifika system exempelvis socialtjänsten eller ekonomisystem har vi identifierat en viss föreliggande säkerhetsrisk, då dessa kräver högre krav av sekretess.

6.4 Hur kan en offentlig verksamhet tillgodose sig nyttan av OpenID?

OpenID finns det för närvarande inget intresse för då detta bygger på webbteknik och kommunernas systemflora till mesta del består av klientbaserade system.

6.5 Vilka aspekter bör beaktas vid användandet av Single Sign-On inom offentlig sektor?

Vi har identifierat följande aspekter: *ekonomiska, organisatoriska, säkerhet och tekniska*.

6.5.1 Ekonomiska

SSO innebär en effektivisering av användar- och lösenordshantering. I en decentraliserad organisation frigörs resurser till annat och i en centraliserad påskyndas hanteringen av behörighet till användaren.

6.5.2 Organisatoriska

Ansvaret för hur användaren hanterar sitt lösenord och användarnamn måste i högre grad läggas på organisationen. Säkerheten kommer inte bli högre vid införandet av SSO, om man inte förändrar rutinerna för hur lösenord ska hanteras. För detta krävs en utbildning så att medvetenhet kring varför lösenord finns till och hur man ska hantera detta. Utbildningen bör innehålla konkreta exempel på vilka konsekvenserna eller följderna kan bli av dålig lösenordshantering.

6.5.3 Säkerhetsmässiga

Lösenordssupporten kommer inte att försvinna bara genom att införa SSO. Därför ser vi andra lösningar för att minska lösenordsproblematiken. Istället för att enbart använda en enkel inloggning bör man använda sig av en tvåfaktorinloggning precis som vissa banker tillämpar. Det kan antingen bestå av både en enklare form av lösenord och fingeravtryck eller pinkod och smart-card, En normal kommun i vår studie har mer än 1000 datorer och att utrusta varje dator med en tvåfaktorslösning blir en ekonomisk betydande kostnad.

6.5.4 Tekniska

Kommuner använder sig av en heterogen systemmiljö och det resulterar i att det är svårt att få systemen att kommunicera med varandra. Systemfloran består både av klient och webbaserade system och detta beror på att en del av systemleverantören inte kan erbjuda webbaserade alternativ. Detta har sin grund i att kommunerna är dåliga på att ställa krav.

6.6 Summering av slutsatserna

De viktigaste slutsatserna vi kan dra av vår studie är att centraliserad och decentraliserad är två olika tillvägagångssätt för användaradministration. Vi har identifierat tre faktorer: helhetsperspektivet, säkerhet och ekonomiska. De aspekterna som vi har identifierat är följande: ekonomiska, organisatoriska, säkerhetsmässiga och tekniska.

6.7 Utvärdering av studien

Vi gjorde ett antagande att kommunerna i någon form använde sig av SSO. Detta har tillbakavisats av kommunerna och respondenterna, dock är ämnet ändå högaktuellt då en kommun är i utvecklingsskedet att införa SSO. Dessvärre för vår del fann vi ingen som idag använder sig av SSO. Om det funnits tid kunde vi haft fler respondenter och utökat antalet kommuner. Detta skulle i sådana fall kunnat inkludera systemägarna eller systemförvaltarnas roll. För att identifiera organisatoriska brister hade vi kunnat använda oss av den kvalitativa metoden observation.

6.8 Framtida forskningsområde

Vi har identifierat tre olika frågeställningar som vore intressant att undersöka vidare.

Vilket av centraliserad eller decentraliserad lösenordadministrering är att föredra inom offentlig sektor ur ett säkerhetsperspektiv?
Vilken är den bästa tvåfaktorsinloggningen att användas tillsammans med SSO för en organisation med begränsade resurser (offentlig sektor)?
Hur kan man på bästa sätt förbättra rutinerna kring hur användarna hanterar sina lösenord?

7. Referenser

Allan, A, 2007, *The Twilight of the Passwords: A Timetable for Migrating to Stronger Authentication*, Gartner http://www.gartner.com/DisplayDocument?ref=g_search&id=501639&subref=simplesearch (kräver prenumeration) Iakttagen: 2008-05-26.

Andersson, B-E, 1985, *Som man frågor får man svar*, Rabén & Sjögren, Kristianstad ISBN10: 91-29-56953-2

Atkinson, R.C. & Shiffrin, R.M, 1968. Human memory: a proposed system and its control processes. In K.W. Spence (ed.), *The Psychology of Learning and Motivation: Advances in Research and Theory, Vol. 2* (pp. 89–195). New York: Academic Press. ISBN10: 0-12-543302-6

Baddeley, A. D, 1998, Working Memory/Mémoire de travail, *C. R. Acad. Sci. Paris, Sciences de la vie / Life Sciences 1998.* 321. 167-173

Baddeley, A. D, Kopelman, M.D. and Wilson, B.A., 2004, *The* Essential *Handbook of Memory Disorders for Clinicians*, John Wiley & Sons, Ltd. ISBN10: 0-470-09141-X.

BankID, 2008a, Förutsättningar http://www.bankid.com/BankidCom/Templates/NormalPage.aspx?id=55&epslanguage=SV Iakttagen 2008-05-27.

BankID, 2008b, Samarbetet kring BankID. http://www.bankid.com/BankidCom/Templates/NormalPage.aspx?id=68&epslanguage=SV Iakttagen 2008-05-20.

Brandell, J, 2008, Allvarligt intrång hos Aftonbladet - lösenordsuppgifter spreds på nätet. http://www.idg.se/2.1085/1.138671 Iakttagen: 2008-05-19

E-legitimation.se, 2008a, Tjänster du kan använda dig av med e-legitimation http://www.elegitimation.se/Elegitimation/Templates/UsingEleg.aspx?id=10 Iakttagen 2008-05-27

E-legtimation.se, 2008b, Hur går det till, http://www.elegitimation.se/Elegitimation/Templates/NormalPage.aspx?id=41 Iakttagen 2008-05-27

Falkcrona, J, 2008, Role-based access control and single sign-on for Web services, Magisteruppsats, Linköping University, Department of Electrical Engineering. http://www.diva-portal.org/diva/getDocument?urn_nbn_se_liu_diva-11224-1__fulltext.pdf Iakttagen 2008-05-26.

Hayday, G, 2002, IT-users in password hell http://news.zdnet.co.uk/itmanagement/0,1000000308,2127377,00.htm Iakttagen: 2008-05-14

Hayday, G, 2003, Counting the cost of forgotten passwords http://news.zdnet.co.uk/itmanagement/0,1000000308,2128691,00.htm?r=1 Iakttagen: 2008-05-14

Jeppsson, P, 2008, Sofi Fahrmans Facebook-sida kapades av hackare http://www.idg.se/2.1085/1.138692 Iaktttagen: 2008-05-19.

Jeräng, M, 2007, Säkerhetsexpert sågade Sapnet i rätten. http://www.idg.se/2.1085/1.103166 Iakttagen 2008-05-14

Kommunallag (1991:900 kap 2 2§) http://www.notisum.se/rnp/SLS/lag/19910900.htm Iakttagen 2008-05-27.

Kotadia, M, 2004, Security Strategy – Gates: The password is dead. http://software.silicon.com/security/0,39024655,39118663,00.htm Iakttagen 2008-05-26

Magoulas, T och Pessi, K, 1998, *Strategisk IT-management*, Göteborgs Universitet, Göteborg

Miller, G A, 1956, The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information, *Psychological Review*, 63, 81-97. http://psychclassics.yorku.ca/Miller/ Iakttagen: 2008-05-26.

Mitrović, P, 2005, *Handbok i IT-säkerhet*, Pagina, Falun ISBN10: 91-636-0841-3

Narine, I, & Neath J.S, 1995, Word-length effects in immediate memory: Overwriting trace decay theory. *Psychonmeic Bulletin & Review*. V 2*(4)* 429-441. http://www2.psych.purdue.edu/~nairne/pdfs/28.pdf . Iakttagen 2008-05-26

Numan, B C & Ts'o, 1995, Kerberos: An Authentication Service for Computer Networks *IEEE Communications Magazine,* Vol. 32, number 9, pages 33-38, September 1994:7. http://gost.isi.edu/publications/kerberos-neuman-tso.html Iakttagen 2008-05-20

OpenID.net, 2008a, What is OpenID? http://openid.net/what/ Iakttagen 2008-05-26

OpenID.net, 2008b, How do I get an OpenID? http://opened.net/get/ Iakttagen 2008-05-26

Open Group, 2001, Single Sign-On http://www.opengroup.org/security/l2-sso.htm Iakttagen: 2008-04-19

Passer, M W. & Smith, R E, *Psychology - The Science of Mind and Behavior*, 4th Ed, Michael W. Passer & Ronald E. Smith, McGraw-Hill Higher Education, Boston ISBN13: 978-0-07-128329-8

Patel, R & Davidsson, B. (2003) Forskningsmetodikens grunder – Att planera, genomföra och rapportera en undersökning, Studentlitteratur, Lund. ISBN13: 978-9144-02288-8

Polisen, Datachippet http://www.polisen.se/inter/nodeid=33380&pageversion=1.jsp Iakttagen 2008-05-24

Recordon, D, Reed, D, 2006, OpenID 2.0: A Platform for User-Centric Identity Management *DIM'06*, November 3, 2006, Alexandria, Virginia, USA http://portal.acm.org/ft_gateway.cfm?id=1179532&type=pdf&coll=GUIDE&dl=GUIDE&CFID=29479275&CFTOKEN=66364303 (kräver prenumeration) ISBN10:1-59593-547-9

Samar,V, 1999, Single Sign-On Using Cookies for Web Applications, http://ieeexplore.ieee.org/iel5/6520/17409/00805192.pdf?tp=&isnumber=&arnumber=805192 Iakttagen 2008-05-26. ISBN10: 0-7695-0365-9

SCB, 2007, *Offentlig ekonomi 2007*. http://www.scb.se/statistik/_publikationer/OE0903_2007A01_BR_OE06SA0701.pdf Iakttagen 2008-05-19. ISBN13: 978-91-618-1367-4

Scienceaid.com, 2007, Multi-store Model.
http://www.scienceaid.co.uk/psychology/cognition/multistore.html Iakttagen 2008-05-18

Skatteverket, 2007, *E-legitimation och Skatteverkets e-tjänster*,
http://www.skatteverket.se/download/18.5c13cb6b1198121ee8580002461/20605.pdf
Iakttagen 2008-05-26.

SKL, 2008, e-ID/e-legitimation.
http://www.skl.se/artikel.asp?C=6504&A=49370 Iakttagen 2008-05-24.

Statskontoret, 2000, *24-timmarsmyndighet - Förslag till kriterier för statlig elektronisk förvaltning i medborgarnas tjänst* (2000:21)
http://www.statskontoret.se/upload/Publikationer/2000/200021.pdf Iakttagen: 2008-05-24

Verva, 2008, http://www.verva.se/verksamhetsstod/it-for-samverkan/elektronisk-identifiering/
Iakttagen 2008-05-27

Wikipedia, 2008, *Active Directory*, http://en.wikipedia.org/wiki/Active_Directory
Senast uppdaterad: 2008-05-20 tid 01:19. Iakttagen: 2008-05-20.

Öhman, A, Nationalencyklopedin: *motivation*
http://www.ne.se.ezproxy.ub.gu.se/jsp/search/article.jsp?i_art_id=259479
Iakttagen: 2008-05-14

Bilaga 1 – Exempelfrågor

IT-ansvariga

- Kan du berätta hur din yrkes- och utbildningsbakgrund ser ut?
- Hur ser er IT-verksamhet ut?
- Vad är din roll i er verksamhet?
- Vilka olika system förfogar kommunen över?
- Vilken form av autentisering använder ni er av?
- Känner du till Single Sign-On?
- Vad är dina tankar kring Single Sign-On?
- Vad är din uppfattning kring lösenord?
- Vilka fördelar ser du med Single Sign-On?
- Vilka nackdelar anser du det finns med Single Sign-On?
- Varför har ni inte infört det?
- Varför införde ni det?
- Kan du berätta hur införandet gick till?
- Hur ser ni på utvecklingen av Single Sign-On inom er verksamhet?
- Känner du till OpenID?
- Vilka rutiner har ni för anställda som slutat?
- Hur många gånger kan man logga på sig utan att det spärras?
- Har ni någon speciell IT-policy?
- Har ni något samarbete med andra kommuner?

Datorsupport

- Kan du berätta lite om din bakgrund?
- Hur ser Er help desk verksamhet ut?
- Vad är din uppgift?
- Vilka olika system använder ni er av i verksamheten?
- Inom vilka områden får ni frågor om?
- Hur ofta får du lösenordsrelaterade frågor? Sker det dagligen?
- Upplever du att det är något problem med lösenord?
- Har det gjorts en studie rörande lösenordsrelaterade problem?
- Hur går det till när en användare glömt av sitt lösenord?
- Vilka rutiner finns när anställda slutar?