

Digitala signaturer – ett alternativ för långsiktigt digitalt bevarande?

Dennis Hiljanen
Kristoffer Ljungqvist

Luleå tekniska universitet

D- uppsats

Data- och systemvetenskap

Institutionen för Industriell ekonomi och samhällsvetenskap

Avdelningen för Systemvetenskap

Förord

Denna studie är utförd inom programmet Data och Systemvetenskap vid Luleå Tekniska Universitet. Efter att ha arbetat många långa dagar och flera nätter är vi nu äntligen färdiga. Vi vill passa på att tacka de respondenter som trots väldigt kort varsel har kunnat ställa upp på intervjuer. Vi vill också tacka vår handledare Lennart Ross för stöd under arbetet med vår studie. Om vi har haft problem har han alltid ställt upp.

Ett speciellt tack går till respektive flickvänner för visad förståelse och stöd under arbetets gång.

Sammanfattning

I denna studie behandlas området långsiktigt digitalt bevarande, med fokus på digitala signaturers lämplighet för autentisering av digitala handlingar. Den teori som beskrivs tar upp vad en digital signatur är, vilka problem dessa har på lång sikt samt konceptet Trusted Archival Services som ett koncept för arkivering av digitala handlingar. Det empiriska materialet har samlats in genom intervjuer med tre valda respondenter. Dessa respondenter har valts utifrån deras praktiska erfarenhet inom detta område.

De slutsatser som har kunnat dras av studien är att digitala signaturer inte är en lämplig teknik för att säkerställa autenticiteten i digitala handlingar på lång sikt. Eftersom det inte finns några vedertagna bättre lösningar för autentisering idag, rekommenderar vi att man bör använda digitala signaturer eftersom det trots allt ger bättre säkerhet än ingenting alls. Man bör också påbörja utvecklingsarbete av nya tekniker för autentisering så fort som möjligt. Detta för att möjliggöra en hållbar lösning för framtiden. I studien kan man se att det är realistiskt möjligt att införa system för hantering av digitala signaturer i en arkivverksamhet. En annan slutsats som har kunnat dras är att TAS är ett väldigt bra koncept för att upprätthålla autenticiteten för de digitala handlingar som arkiven har hand om, men att konceptet också har vissa delar som arkiven bör tänka över innan ett införande av det.

Abstract

In this thesis the subject long-term digital preservation is considered. The focus is on how appropriate digital signatures are for authentication of digital records. The theory used describes what a digital signature is, what long-term problems they suffer from and Trusted Archival Services, which is a concept for how to archive digital records. The empirical material was collected through interviews with three chosen respondents. These respondents have been chosen from their practical experiences within this area.

The conclusions that have been drawn in this thesis show us that digital signatures aren't a suitable technique for securing authenticity within digital records in a long time-span. Since there are no better solutions for authentication today that have been accepted, we still recommend the use of digital signatures for the time being. After all they give better security than using no authentication-technique at all. Furthermore, development of new authentication-techniques should start as soon as possible to maintain a lasting solution for the future. In the thesis, we can also see that it's realistic to implement systems for management of digital signatures in archives. Another conclusion that have been pointed out in this thesis is that Trusted Archival Services is a very good concept for maintaining authenticity for digital records that the archives keep, but Trusted Archival Services has some parts that should be thought over by the archives before implementation.

1. Introduktion	1
1.1. Bakgrund.....	1
1.2 Problembeskrivning.....	1
1.3 Forskningsfrågor	3
1.4 Syfte.....	3
1.5 Avgränsningar.....	3
1.6 Definitioner	3
2. Teori.....	5
2.1 Digitala arkivhandlingar	5
2.1.1 Problem med digitala arkivhandlingar.....	5
2.2 Vad är en digital signatur?	6
2.2.1 Vilka tekniker för autentisering existerar?.....	7
2.2.2 Problem med digitala signaturer inom långsiktigt digitalt bevarande.....	9
2.3 System för digitala signaturer.....	10
2.4 Trusted archival services.....	10
3. Metod.....	13
3.1 Vetenskapligt förhållningssätt	13
3.2 Forskningsansats	13
3.3 Typ av studie.....	14
3.4 Kvantitativ kontra kvalitativ.....	14
3.5 Datainsamlingsmetod	15
3.5.1 Intervjuer	15
3.5.2 Intervjuguide.....	16
3.6 Urval av respondenter.....	16
3.7 Analysmetod	17
3.8 Validitet och reliabilitet	17
4. Empiri	18
4.1 Intervju med Göran Kristiansson på Riksarkivet.....	18
4.1.1 Digitala signaturer i arkivsystem.....	18
4.1.2 Digitala signaturer i samband med långsiktigt digitalt bevarande.....	18
4.1.3 Trusted Archival Services.....	19
4.2 Intervju med Lars-Erik Hansen på TAM-arkiv	20
4.2.1 Digitala signaturer i arkivsystem.....	20
4.2.2 Digitala signaturer i samband med långsiktigt digitalt bevarande.....	20
4.2.3 Trusted Archival Services.....	21
4.3 Intervju med Magnus Wählberg på Skatteverket.....	22
4.3.1 Digitala signaturer i arkivsystem.....	22
4.3.2 Digitala signaturer i samband med långsiktigt digitalt bevarande.....	22
4.3.3 Trusted Archival Services.....	23
5. Analys och Diskussion	24
5.1 Digitala signaturer i arkivsystem	24
5.2 Digitala signaturer i samband med långsiktigt digitalt bevarande.....	26
5.3 Trusted Archival Services	27
6. Avslutning.....	29
6.1 Slutsatser.....	29
6.1.1 Digitala signaturer – en lämplig teknik?.....	29
6.1.2 Realistiskt möjligt att implementera?.....	30
6.1.3 Trusted Archival Services – ett bra koncept?.....	30
6.1.4 Diskussion om slutsatser	31
6.2 Fortsatt forskning	32
6.3 Metoddiskussion.....	32
6.3.1 Teori.....	32
6.3.2 Undersökningsobjekt.....	32
6.3.3 Intervjufrågor.....	32
6.3.4 Slutsatser	33
7. Referenslista	34
7.1 Bokreferenser	34
7.2 Internetreferenser.....	34
8. Bilagor.....	37
8.1 Intervjuguide.....	37

1. Introduktion

I vår introduktion kommer vi att ge en beskrivning av området långsiktigt digitalt bevarande. Vi kommer börja med en bakgrund som följs av en problembeskrivning. Sedan presenterar vi våra forskningsfrågor, vårt syfte med rapporten samt de avgränsningar vi har gjort.

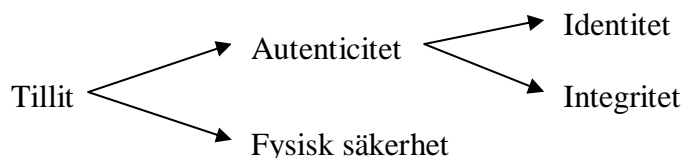
1.1. Bakgrund

Dagens snabba tekniska utveckling leder till en allt större mängd digitaliserad information i våra system. Denna information, mjukvaran och hårdvaran den lagras på föråldras snabbt till följd av att ny teknik utvecklas hela tiden. Enligt Arkivutredningen (2000) kan vi inte med nuvarande metoder och tekniker bevara denna information långsiktigt på ett kostnadseffektivt sätt. De menar att viktig information kommer gå förlorad om ingenting händer inom området. Detta leder till att nya metoder och tekniker måste tas fram för att kunna bevara digitaliserad data långsiktigt. Långsiktigt digitalt bevarande innebär hur man bevarar digitaliserad data på bästa sätt över en lång tid utan att den försvinner eller ändras. Detta område är relativt nytt och innebär ett stort problem för informationsbevarande ur ett långsiktigt perspektiv. Därför utförs forskning i hela världen för att få fram optimala lösningar för ett långsiktigt digitalt bevarande (Arkivutredningen, 2000). Det finns alltså flera olika frågor som bör utredas inom detta område.

1.2 Problembeskrivning

Några som kommer att beröras väldigt mycket av långsiktigt digitalt bevarande är arkivmyndigheterna i världen. De tillhandahåller inte bara information för dagens medborgare utan även för framtiden. Att bevara och tillgängliggöra alla olika typer av digitala handlingar som förekommer inom den offentliga förvaltningen är en övergripande målsättning som arkivmyndigheterna har (Arkivutredningen, 2000). Detta gör att arkivmyndigheterna har stora krav på sig att upprätthålla största möjliga tillgänglighet och tillit till handlingarnas äkthet.

Ett stort problem vid långsiktigt digitalt bevarande är att kunna uppnå tillit till den information som lagras. Tilliten byggs upp av informationens autenticitet samt dess fysiska säkerhet. Autenticitet kan därefter delas upp i identitet och integritet på följande sätt (Runardotter et. Al., 2005):



Figur 1. Illustrering av begrepp, egengjord figur över kategorisering.

Identitet innebär att det är möjligt att se all information om när data skapades och av vem. Det här är viktigt för att slutanvändaren ska kunna se vem upphovsmannen till en digital handling är och när handlingen har skapats. Integritet innebär att datan inte ändrats efter att upphovsmannen publicerade materialet. Det är viktigt att slutanvändaren ska kunna se att datan inte har förfalskats sedan den lagrades. Det finns dock problem med att säkerställa integriteten i arkivsystem. Den tekniska utveckling som har skett av

hårdvara och mjukvara har gjort att det finns många olika format. Dessa format är inte alltid kompatibla mellan olika versioner av mjukvara och olika plattformar. Det här leder till att mycket av det material som finns i digital form och producerats för bara några år sedan inte går att läsa med dagens mjukvara. Information kan gå förlorad på detta sätt och isåfall påverkas även informationens integritet negativt vilket givetvis leder till att man inte kan lita på att den information som presenteras är oförändrad. Tillgängligheten i systemen påverkas även negativt när man inte kan säkerställa att informationen finns kvar. Om både identiteten och integriteten är hög innebär det att autenticiteten är hög (Runardotter et. Al., 2005).

Enligt Arkivutredningen (2000) har arkivmyndigheterna en stor möjlighet att hantera frågan om tillit till dess handlingar genom att dra nytta av den utveckling som har skett inom till exempel e-handel. För att lösa problemet med autenticitet inom e-handel har man ofta använt sig av såkallade digitala signaturer. De digitala signaturerna har fungerat väldigt bra för att höja autenticiteten på digitalt material och denna typ av signaturer har också nämnts som ett möjligt tillvägagångssätt vid långsiktigt digitalt bevarande. En digital signatur innebär kortfattat en sorts digital stämpel på en publikation som verifierar att det är upphovsmannen som faktiskt skrivit den. En digital signatur kan också användas till att säkerställa att information inte har förändrats under tiden informationen har lagrats.

Allt är dock inte positivt med digitala signaturer. Det finns många frågetecken kring användandet av digitala signaturer som måste utredas innan man kan ta ställning till om det är en bra teknik för långsiktigt digitalt bevarande. Det har nämnts att digitala signaturer i kombination med långsiktigt bevarande innebär vissa problem eftersom digitala signaturer har en begränsad livslängd. Framförallt är det frågor om hur äkthetscertifikatshantering och krypteringsnyckelshantering ska ske som innebär problem vid användning av digitala signaturer.

The European Electronic Signature Standardization Initiative (2000) visar på ett koncept kallat TAS, trusted archival services, som är skapat för att kunna eliminera dessa långsiktiga problem med digitala signaturer.

Eftersom frågorna om handlingars autenticitet och människors tillit till dessa handlingar är viktiga frågor inom området långsiktigt digitalt bevarande tycker vi att det vore intressant att utreda om dagens digitala signaturer tillåter en hög autenticitet vid långsiktigt digitalt bevarande. Vi känner också att det finns andra kriterier som inverkar vid ett val av digitala signaturer som autenticeringsmetod, nämligen, hur enkelt systemet är att implementera, hur mycket det kostar att använda och hur enkelt det är att använda när det väl är på plats, vilket gör att även detta blir intressant för oss att utreda. Att detta är relevanta kriterier bekräftas av Nielsen (2001) som menar att enkelheten i ett system alltid vinner över komplexiteten. Han menar att ju enklare ett system är att använda desto mindre förändringar krävs av ett system i slutändan vilket leder till minskade kostnader för organisationer. Strävan efter kostnadseffektivitet är enligt Friedman och Cornford (1989) viktigt för företagen, framförallt på ledningsnivå. Organisationer vill ha högre kvalitet till lägre kostnader. Vidare menar Werr et. Al. (1995) att eftersom ett införande ett IS innebär stora sociala förändringar i en verksamhet är det viktigt att det är så enkelt som möjligt att införa. Den sista faktor vi skulle vilja undersöka i denna studie är konceptet TAS. TAS är ju tänkt att hjälpa till vid autenticering av digitala handlingar och vi undersöker gärna om det är ett bra val att införa i verkligheten. Vi har

också sett att det finns en uttalad önskan om mer forskning på området digitala signaturer i kombination med långsiktigt digitalt bevarande, vilket får området att kännas ännu mer aktuellt för oss att utreda.

1.3 Forskningsfrågor

Våra forskningsfrågor lyder:

- Är det realistiskt att använda sig av digitala signaturer i arkivsystem med avseende på implementation, användbarhet och kostnadseffektivitet?
- Är digitala signaturer en lämplig teknik för att tillhandahålla en hög autenticitet i digitala handlingar på lång sikt?
- Är trusted archival services ett bra koncept för att eliminera de problem som digitala signaturer har vid långsiktigt digitalt bevarande?

1.4 Syfte

Vi vill utreda om digitala signaturer är en lämplig teknik för att kunna bevara en hög autenticitet på digitala handlingar när dessa bevaras på lång sikt. Vi vill utreda detta för att digitala signaturer ofta har föreslagits som en teknik vid långsiktigt bevarande av digitala handlingar, eftersom att detta inte riktigt har utretts ordentligt tidigare. Vi vill även undersöka hur andra aspekter än autenticiteten i digitala handlingar upplevs, nämligen kostnadseffektivitet, enkelhet att införa och användbarhet. Detta för att det är viktiga faktorer att ta hänsyn till. Det talas även ofta om att digitala signaturer har en kort livslängd och att det därför ofta uppstår problem vid långsiktigt digitalt bevarande med hjälp av dessa. Trusted archival services är ett koncept som har utvecklats för att motverka vissa av dessa problem och därför vill vi även utreda om det är en tänkbar lösning att använda sig av i framtiden för de arkiv som existerar idag.

1.5 Avgränsningar

Vi kommer att avgränsa oss till att endast ta hänsyn till digitala handlingar som inte får förändras efter att de har hamnat i ett digitalt arkiv. Vi har valt att studera hur autenticiteten i digitala handlingar bibehålls på lång sikt med hjälp av digitala signaturer, men har valt att utelämna den fysiska säkerheten. Det är helt enkelt omöjligt i vår studie att dra några slutsatser av att jämföra fysisk säkerhet med digitala signaturer eftersom de digitala signaturerna inte stödjer fysisk säkerhet på något sätt.

1.6 Definitioner

Vår rapport riktar sig till personer med insikt i långsiktigt digitalt bevarande. Trots detta har vi valt att definiera några centrala begrepp för att undvika missförstånd.

Arkiv

Vi definierar ett arkiv som en samling av pappershandlingar. Vi förutsätter att arkiven drivs av organisationer, institutioner eller bibliotek. Vanliga arkiv tillhandahåller dessutom extra tjänster för slutanvändaren, till exempel sökning i arkiven.

Digitala arkiv

I vår studie definierar vi ett digitalt arkiv precis som ett vanligt arkiv förutom att det är digitaliserat. Vi förutsätter att de digitala arkiven drivs av organisationer, institutioner eller bibliotek precis som idag.

Digitala arkivhandlingar

I vår undersökning definierar vi digitala arkivhandlingar som en vanlig pappershandling. Den digitala arkivhandlingen kan vara vilken typ av dokument som helst, exempelvis bilder, dokument, musik.

2. Teori

*I vår teori kommer vi att ge en beskrivning av vad digitala arkivhandlingar innebär samt vilka problem som existerar i digitala arkiv. Sedan förklarar vi vad en digital signatur är och vilka olika typer av digitala signaturer som existerar. Under denna punkt ställer vi även upp variabler som vi anser vara relevanta i sammanhanget. Vi fortsätter sedan med att visa vilka problem dessa digitala signaturer har i samband med långsiktigt digitalt bevarande. Sist i teoriavsnittet avhandlar vi vad konceptet, *Trusted archival services*, innebär och hur detta koncept kan lösa de problem som uppstår vid långsiktigt digitalt bevarande med hjälp av digitala signaturer.*

2.1 Digitala arkivhandlingar

Digitala arkivhandlingar har samma syfte som pappershandlingar, att lagra information, men det finns skillnader. Den fundamentala skillnaden är att digitala handlingar förmedlas med hjälp av teknologi vilket betyder att rätt kombination av hård- och mjukvara krävs för att man ska kunna ta del av den digitala handlingen. Handlingen kan endast tas del av så länge teknologin och datan kan interagera. Digitala arkivhandlingar är alltså inte fysiska objekt som pappershandlingar är, utan resultatet av förmedlingen mellan teknologi och data (Heslop, Davis & Wilson, 2002).

Enligt Heslop et. al. (2002) är originalitet ett viktigt begrepp för att pappershandlingar ska ha en hög autenticitet. Detta gäller däremot inte för digitala handlingar eftersom många användare kan titta på samma objekt samtidigt och uppleva samma sak. Vid varje visning av en digital handling, det vill säga varje gång en handling öppnas, blir handlingen en ny originalkopia av sig själv (Heslop, Davis & Wilson, 2002). När det gäller digitala arkivhandlingar är det väldigt viktigt att upplevelsen blir densamma oavsett var och när handlingen öppnas. Med andra ord ska handlingen alltid se likadan ut som den gjorde när den skapades.

Relationen mellan digitalt bevarande och autenticitet är meningsfullt bevarande, det vill säga hur användbart det man bevarar är. Målet med bevarande är att ge framtida användare möjligheten att återfå, ha tillgång till, tolka, visa, förstå samt uppleva handlingar på ett meningsfullt och giltigt sätt. Just nu finns det ingen gångbar långsiktig strategi för att försäkra att digital information kommer att vara läsbar i framtiden. Svårigheten att definiera en gångbar strategi för långsiktigt digitalt bevarande beror bland annat på att vi inte lyckas förstå och uppskatta problemen med autenticitet (Rothenberg, 2000).

2.1.1 Problem med digitala arkivhandlingar

För att förlänga livslängden på information i ett digitalt arkiv är det viktigaste, enligt RLG och OCLCs rapport, *"Trusted Digital Repositories: Attributes and Responsibilities"*, att hantera följande frågor om arkivet där handlingarna lagras:

- Identitet – Arkivet måste tillhandahålla information om vem upphovsmannen till en digital handling är, när handlingen är skapad, varför den är skapad och i vilka sammanhang den har använts (Hofman, 2003).

- Integritet – En hög integritet är viktigt att ha i arkiven för att kunna garantera att handlingarna är oförändrade medan de är lagrade.

Enligt Dobratz och Schoger (2005) byggs användarnas tillit till digitala arkivhandlingar upp av autenticitet. Det finns ingen generell definition av vad autenticitet egentligen betyder, varje disciplin har sin egen syn på vad det är. Dess mening är inte bara att verifiera upphovsmannen av en handling, utan autenticitet behandlar även ämnen som integritet, fullständighet, korrekthet, validitet, tilltro till ett original, meningsfullhet samt hur ändamålsenligt det är (Rothenberg, 2000). Dobratz och Schoger (2005) delar upp autenticitet i delarna identitet och integritet. Vidare anser de att om autenticiteten är hög och säkerheten är hög i ett digitalt arkiv, blir användarnas tillit till det digitala arkivet och de handlingar det lagrar hög. För att ytterligare höja användarnas tillit till arkiven anser de att arkiven bör sträva efter att bli certifierade på något sätt.

Digitala arkiv har alltså som uppgift att bevara digitala handlingar. Att bevara digitala handlingar i sitt originalskick, det vill säga i det format som den skapades i, innebär inget problem idag. Däremot kommer dagens digitala handlingar att byta format förr eller senare och det är då väldigt viktigt att kunna verifiera att handlingen är äkta även efter bytet av format (Heslop, Davis & Wilson, 2002). Detta leder ofta till problem med autenticiteten för den digitala handlingen tack vare att vi idag inte har några bra tekniker för att få en hög autenticitet vid långsiktigt digitalt bevarande.

En av de lösningar som föreslås för att säkerställa en handlingens autenticitet är digitala signaturer. Digitala signaturer används ofta inom området elektronisk handel för att säkerställa att information är oförändrad samt för att verifiera att informationen kommer från rätt person (Lynch, 1999). Han menar också att digitala signaturer kan användas inom långsiktigt digitalt bevarande för att säkerställa både informationens identitet samt integritet.

InterPares Authenticity Task Force har en motsatt ståndpunkt enligt Dumortier och Van den Eynde (2005). De anser att digitala signaturer inte är en lämplig teknik att använda för autenticering av digitala handlingar inom långsiktigt digitalt bevarande. De menar att tekniken i sig har utvecklats för kommunikation, exempelvis E-post, vilket gör att signaturerna har en kort livslängd. De är helt enkelt baserade på algoritmer som kan knäckas i framtiden.

2.2 Vad är en digital signatur?

En digital signatur är, precis som en vanlig signatur, ett sätt att identifiera sig själv med och samtidigt godkänna innehållet i till exempel en handling. Den digitala signaturen möjliggör även att den som har skapat en handling inte kan förneka det vid ett senare tillfälle (Regeringskansliet, 1998). Den stora skillnaden är givetvis att den digitala signaturen skapas på en dator.

Idag är digitala signaturer juridiskt bindande under förutsättning att man kan påvisa signaturens äkthet och att handlingen inte har förvanskats. Det ställer givetvis stora krav på att digitala signaturer ska klara av att identifiera vem som har skrivit eller godkänt handlingen samt att handlingens integritet ska kunna garanteras. Informationen i handlingen ska vara oförändrad och i samma utförande som när den signerades. För att lösa detta finns det, i dagsläget, några olika tekniker för att kunna autenticera en digital

handling. Gemensamt för dessa tekniker är att de strävar efter att man ska kunna verifiera att det är rätt person som har signerat handlingen och att informationen är oförändrad (Regeringskansliet, 1998).

2.2.1 Vilka tekniker för autentisering existerar?

Kryptering med hashsummer

Ett populärt sätt för upphovsmannen till en digital handling att visa att det är han som är upphovsman är en digital signatur som skapas med hjälp av assymetrisk kryptering. För att användaren sedan ska se att informationen är oförändrad kan man använda sig av en hashsumma.

Linder (2003) beskriver processen med att skapa en digital signatur. Han menar att personen som vill skapa signaturen först gör ett såkallat kondensat av den information som ska skickas eller lagras. Att göra ett kondensat innebär att man använder en algoritm för att skapa en ny textsträng av informationen, en hashsumma. Hemligheten med att använda sig av hashsummer är att den nya textsträngen alltid blir likadan vid ett likadant meddelande, men en helt annan textsträng om någon bit av informationen är olik. Det går inte heller att via textsträngen räkna baklänges för att se vad för algoritm som används. När man sedan i framtiden vill kontrollera att informationen är oförändrad tar man och använder samma algoritm som användes och räknar ut en ny textsträng. Om textsträngarna matchar är informationen oförändrad. Hashsignaturer är alltså väldigt säkra när man försöker fastställa integriteten i ett meddelande eller i en lagrad digital handling (Linder, 2003).

Det räcker dock inte att bara kunna garantera integriteten i en digitalt lagrad handling för att användare ska kunna känna tillit till handlingen. Digitala signaturer måste även kunna visa vem som är upphovsman till verket eller vem som går i god för verket. Ett sätt att lösa detta problem är med hjälp av assymetrisk kryptering. I exemplet tidigare har upphovsmannen redan skapat ett kondensat med hjälp av sin digitala handling. Han vill nu kunna garantera att det är han som har skapat verket och tar då och använder en krypteringsalgoritm som har skapats av Rivest, Shamir och Adleman (1978) och som används i så gott som alla assymetriska krypteringssystem idag på grund av dess säkerhet.

Med hjälp av denna algoritm tar upphovsmannen och skapar en privat och en publik krypteringsnyckel. Med hjälp av den privata nyckeln (krypteraren) kan upphovsmannen kryptera hashsumman. Det enda som kan dekryptera hashsumman nu är den publika nyckeln (dekrypteraren) som alla har tillgång till. Med hjälp av den publika nyckeln kan man nu dekryptera hashsumman för att se att det är upphovsmannen med rätt privat nyckel som har signerat dokumentet (Rivest, Shamir & Adleman, 1978). För att man ska veta vem som äger en privat nyckel finns det vissa certifieringsorgan som tillhandahåller information om vem som äger en nyckel.

Tillsammans använda gör hashsummer och assymetrisk kryptering att både identiteten och integriteten kan garanteras i en digitalt lagrad handling, vilket gör att slutanvändarens tillit till den digitala handlingen bör vara hög.

Vattenmärkning

Grundtanken med att använda sig av såkallad vattenmärkning är att själva märket ska vara ett skydd mot förfälskningar, men att märket också ska kunna identifiera upphovsmannen till verket. Istället för att använda sig av en digital signatur för autenticering är det tänkt att man bakar in ett meddelande direkt i handlingen för att på så sätt ha all information om upphovsmannen etcetera i verket. Om någon manipulerar en vattenmärkt handling, är det tänkt att handlingen ska förstöras, alternativt att vattenmärket förstörs (Wickström, 2004). Ett vattenmärke ska helt enkelt vara ett skydd som är svårt att kringgå. Ett vattenmärke kan även fästas på flera olika typer av digitala objekt, allt från bilder, ljud och video till databaser, 3D-strukturer och textfiler.

När man vattenmärker en digital handling fäster man helt enkelt ett litet meddelande till handlingen. Som exempel kan tänkas att det i en text placeras ut upphovsmannen av texten i bitströmmen av handlingen. För att göra vattenmärkningen säkrare kan man placera ut flera meddelanden i hela handlingen. Wickström (2004) menar dock att ett vattenmärke i en digital handling alltid försämrar kvaliteten på handlingen eftersom man lägger till extra information i handlingen för att skapa ett vattenmärke. Wickström (2004) menar också att det är en avvägning man måste göra när man tar ställning till att använda sig av vattenmärkning som metod. Dessutom försämras kvaliteten på den digitala handlingen mer ju säkrare man vill att handlingen ska vara.

När man talar om vattenmärkning finns det två olika typer av vattenmärkning:

- Robust vattenmärkning – Används för att garantera att ett objekt inte kan förändras för mycket utan att det förstörs, används oftast vid vanlig sedelvattenmärkning.
- Fragil vattenmärkning – Används för att kunna autenticera ett objekt. Fragila vattenmärken är väldigt känsliga och tanken är att vattenmärkningen ska försvinna direkt vid en förändring i det vattenmärkta materialet. Används oftast vid digital vattenmärkning.

Den robusta vattenmärkningen innebär bland annat att man vill att meddelandet ska vara intakt så länge inte den digitala handlingen modifieras alltför mycket. När man använder robust vattenmärkning vill man även att handlingen ska överleva olika formatkonverteringar utan att förstöra vattenmärkningen.

Den fragila vattenmärkningen däremot används ofta för att ge hög autenticitet åt en handling. Wickström (2004) nämner en digitalkamera som exempel. Där märker digitalkameran upp en bild genom att lägga till en datummarkering för att man senare ska kunna säkra att bilden inte är manipulerad.

När man ska välja en av dessa metoder bör man först ta hänsyn till vilken som passar bäst för det man ska lagra. Eftersom den robusta vattenmärkningen är utvecklad för att vara säkrare genererar den också fler falska alarm vid vattenmärkesdetektionen (Wickström, 2004). Wickström (2004) påstår också att det är väldigt vanligt att attacker inriktar sig direkt på vattenmärkningen och försöker att ta bort den från handlingen.

2.2.2 Problem med digitala signaturer inom långsiktigt digitalt bevarande

Som tidigare visats finns det problem med att lagra digitala handlingar. Den autenticitet som ett arkiv kan tillhandahålla på sina digitala handlingar har betydelse för den tillit användarna känner till arkivet. Detta autenticitetsproblem kan delvis lösas med hjälp av digitala signaturer. Däremot finns här ett stort problem när det gäller långsiktigt digitalt bevarande. Eftersom man pratar om obestämda tidsperioder är det viktigt att lösningarna fungerar så länge som möjligt.

Lynch (1999) menar att det finns några problem med att använda digitala signaturer för att autentisera ett verk i de digitala arkiven på lång sikt. Han pekar på att digitala signaturer bara fungerar tills dess att en digital handling måste byta format till exempel på grund av att ny it-teknik börjar användas. Eftersom till exempel en hashsumma beräknas på en exakt informationsmängd blir inte den nya textsträngen likadan om man beräknar den på den nya informationen efter ett formatbyte. En digitalt signerad handling måste också kunna signeras om efter ett visst tag för att kunna behålla sin autenticitet. Andra problem som nämns är att det kan tänkas att upphovsmannen inte finns tillgänglig alternativt inte är villig att signera om sitt verk igen (Lynch, 1999). Det här visar att digitala signaturer har problem vid bevaring på lång sikt. En högst giltig fråga är hur man bör gå tillväga efter att livslängden har gått ut?

Lekkas och Gritzalis (2004) menar att det är ett stort hopp mellan långsiktigt digitalt bevarande av digitala handlingar och långsiktigt digitalt bevarande av digitala signaturer. Där digitala handlingar oftast har problem som rör dess läsbarhet över tiden menar författarna att digitala signaturer bland annat har följande problem:

- Eftersom sannolikheten att en kryptering knäcks ökar över tiden betyder det att den digitala signaturen blir osäkrare ju längre tid som går, vilket också leder till att digitala signaturer borde signeras om under vissa bestämda tidsintervaller, helst med nya krypteringsnycklar. Lekkas och Gritzalis (2004) menar att en tänkbar lösning på detta problem kan vara med hjälp av certifieringsorgan som bara tillåter krypteringsnycklar att vara högst två år gamla innan dessa måste bytas ut.
- De krypteringsnycklar som används vid signering av en digital handling kan knäckas innan deras tidsperiod är slut vilket gör att vem som helst kan modifiera den digitala signaturen.
- Att ta reda på vem som äger en privat nyckel genom att kontakta ett certifieringsorgan kanske inte är tillämpligt i framtiden. Vad finns det då för lösningar för att ta reda på vem som har signerat en digital handling? Om det dessutom inte finns något certifieringsorgan kvar går det alltså inte att ta tillbaka ett certifikat från någon och då kan den personen förfalska den signaturen.
- Den tredje part som tillhandahåller information om olika certifikat och privata nycklar kanske inte kan lita på i framtiden tack vare att de inte fullföljer de krav som de har på sig längre. Det kan även tänkas att de har lagt ner sin verksamhet och då uppstår samma problem igen, hur kan man lita på att ett digitalt certifikat för en privat nyckel faktiskt stämmer?

Trots att digitala signaturer är ett effektivt och välanvänt sätt vid meddelandehantering inom elektronisk handel samt vid lagring av digitala handlingar idag är allt detta stora problem som måste lösas för att digitala signaturer ska kunna användas effektivt vid

långsiktigt digitalt bevarande. Om hashsummer slutar fungera på lång sikt kan vi inte garantera att information är oförändrad och om krypteringsnycklar eller certifikat slutar fungera kan vi inte garantera att avsändaren, det digitala arkivet eller upphovsmannen är vilka de utger sig för att vara.

2.3 System för digitala signaturer

När en organisation ska bestämma sig för att införa digitala signaturer i sin verksamhet finns det ett antal kriterier som inverkar. Dessa kriterier är hur enkelt systemet är att implementera, hur mycket det kostar att använda och hur enkelt det är att använda när det väl är på plats.

Kostnadseffektivitet

Runardotter (2007) skriver att det är viktigt för arkiven att ta väl hand om det arkiverade materialet. Hon visar att det finns pengar att spara om man har ett välorganiserat arkiv. Ett välstrukturerat arkiv gör att man kan hämta handlingar effektivare och enklare och därmed sparar man pengar på detta. Runardotter (2007) menar att andra fördelar med system för digital verksamhet är att det ger spårbarhet samt säkrar det sociala och kulturella arvet. Att använda standardsystem är generellt sett mindre kostsamt än att utveckla nya system från grunden (Sundgren, 2003). Han menar även att de ofta är mer beprövade och därmed driftsäkrare vilket också leder till ett mer kostnadseffektivt system.

Enkelhet att använda

Axelsson, Fihn, Rosenqvist (2003) menar att dagens system för digitala signaturer är väldigt enkla att använda. De visar att systemen sköter autentiseringen av de digitala handlingarna per automatik.

Enkelhet att införa

Det finns vissa problem som kan uppstå vid införande av ett standardsystem i en organisation. Morisio et. Al. (2006) menar att standardsystem inte går att anpassa fullt ut, att kunden inte anpassar sina processer till att passa systemet. Andra problem är att mindre företag ofta visar sig vara mer beroende av leverantören och inte kan sköta systemet själv. Att det genomförs otillräcklig utbildning kan också leda till problem vid införande av dessa system (Morisio et. Al., 2002).

2.4 Trusted archival services

The European Electronic Signature Standardization Initiative (EESSI) har föreslagit ett koncept för digitala arkiv som ska garantera att digitala signaturer kan bli bevarade på väldigt lång sikt med hög autentisitet. Detta koncept kallas Trusted Archival Services (TAS). Kravet på att en digital handling eller digital signatur ska kunna bevaras på lång sikt gör att följande faktorer måste behandlas av ett arkiv som vill vara ett TAS (Dumortier et. Al., 2000):

Handlingarnas format

Ett arkiv ska endast acceptera arkivhandlingar vars format kan valideras längre fram. Detta betyder att handlingens format ska vara känt då handlingen skickas till det digitala arkivet. Alla typer av format är inte acceptabla men bör åtminstone uppfylla kravet "WYSIWYS" vilket betyder What You Sign Is What You See. Detta betyder att man måste kunna se och tolka vad man ska signera med blotta ögat.

Varje arkiv som vill bli ett TAS ska publicera en lista på de olika filformat som arkivet stödjer. Det är upp till varje arkiv att välja vilka filformat som ska stödjas samt att garantera att intern kompatibilitet med dessa format existerar. Varje arkiv ska kontrollera filformatet för varje digital handling innan dessa accepteras för arkivering.

Teknologisk Interoperabilitet

Ett arkiv ska endast acceptera arkivhandlingar som har en redan validerad signatur. Om det är nödvändigt ska ett arkiv även samla utförligare information för att kunna garantera validering på lång sikt. Ett arkiv ska även kunna garantera interoperabilitet i de fall olika format för signaturer finns tillgängliga. Alltså ska också acceptabla format för signaturer kontrolleras innan arkivering. Om signaturen har ett giltigt format för handlingen den används på kan arkivet arkivera handlingen. Det är även här upp till varje arkiv att välja vilka typer av format på signaturer de ska stödja.

Bakåtkompatibilitet

Ett digitalt arkiv som vill bli ett TAS ska erbjuda bakåtkompatibilitet. Detta innebär att arkivet ska behålla både hård och mjukvaruplattformar för att kunna visa de digitala handlingarna i framtiden. Om inte detta kan göras ska arkivet istället ha en emulator för att kunna använda de digitala handlingarna i framtiden även om inte teknologin finns tillgänglig.

Kryptografisk uppföljning

Ett arkiv ska kontinuerligt tidsstämpla arkiverade handlingar med hjälp av starka algoritmer för att kunna garantera långsiktig validering av dessa handlingar. Arkiven ska göra detta till exempel, en gång om året eller när en krypteringsalgoritm knäcks. Ett arkiv ska inte bara följa utvecklingen av de olika kryptografiska algoritmerna, utan också ta hänsyn till hur bra dess implementation varit i applikationer för signering. Alltså ska ett arkiv som vill bli ett TAS inte bara skydda mot algoritmer som inte fungerar utan även buggar och dåliga implementationer av dessa för att kunna upprätthålla en pålitlig service.

TAS Modeller

Det finns två olika modeller som konceptet TAS följer för lagring av digitala handlingar, den centraliserade modellen eller den distribuerade modellen.

Centraliserad modell

I denna modell lagras redan signerade digitala handlingar i ett TAS. En digital handling skickas åt gången och blir lagrad oberoende av andra dokument i ett TAS. I och med detta kan användaren lita på att både handlingen och signaturen blir bevarad. Den centraliserade modellen är designad som en online lösning. Tanken är att användare ska kunna skicka signerade handlingar online till ett TAS för arkivering med hög tillit. I denna modell är identifikationen av dokument viktiga för att kunna erbjuda en tillförlitlig modell för användarna. Hur identifieringen ska gå till ska specificeras av varje enskilt TAS och ska åtminstone erbjuda en unik identifierare till användaren. En annan viktig del i denna modell är handlingens autentisering eftersom dessa inte lagras hos användaren. Även här bör ett TAS specificera hur denna autentisering bör gå till där kravet är att endast tillåta personen eller personerna som skickat in det signerade dokumentet att hämta hem samma dokument.

Distribuerad modell

I den distribuerade modellen lagrar användaren själv sina handlingar, det är bara signaturen som lagras i ett TAS. En digital signatur skickas åt gången och blir lagrade oberoende av andra signaturer i TAS. Fördelen med denna modell är möjligheten att applicera en digital signatur på alla olika typer av handlingar, inklusive krypterade och komprimerade handlingar. Eftersom arkiven inte behöver ta emot annat än den digitala signaturen kan man använda sig av starkare krypteringar som inte använder beräkningskraft av TAS utan av den organisation som vill skicka in den digitala handlingen.

3. Metod

I det här kapitlet beskriver vi grundläggande hur ett forskningsarbete kan läggas upp, samt vårt val av tillvägagångssätt.

3.1 Vetenskapligt förhållningssätt

Det finns två stycken vetenskapliga förhållningssätt som används inom forskning:

- Hermeneutik – Tolkningslära.
- Positivism – Mätbara statistiska samband.

Hermeneutik innebär att man försöker förstå och tolka människors handlingar, ordet betyder ”allmän tolkningslära”. När en forskare utför forskning med ett hermeneutiskt förhållningssätt brukar det vara vanligt att göra intervjuer. Utifrån dessa intervjuer försöker man tolka svaren för att försöka dra slutsatser därifrån. Detta förhållningssätt svarar ofta på frågan varför något ser ut på ett viss sätt.

Positivism är ett mer naturvetenskapligt förhållningssätt där målet är att finna lagbundenheter. Resultatet som man får vill man kunna beskriva i siffror, till exempel statistik. (Andersson, 1979)

Eftersom vi i vår studie ska använda oss av intervjuer för att ta reda på om digitala signaturer är ett bra alternativ för långsiktigt digitalt bevarande kommer vi att använda oss av det hermeneutiska förhållningssättet. Motiveringen är att det troligtvis är svårt att göra någon statistisk undersökning på detta, vi vill ha ganska djupa svar på våra frågor eftersom ämnesområdet inte är riktigt utrett ännu. Dessutom kommer vi att ställa följdfrågor och måste tolka svaren på dessa frågor, vilket gör att det hermeneutiska förhållningssättet passar utmärkt för vår undersökning.

3.2 Forskningsansats

Inom all forskning försöker man få fram nya slutsatser. För att få fram dessa slutsatser tar man hjälp av en forskningsansats i sitt arbete, helt enkelt ett tillvägagångssätt för att kunna dra slutsatser. Patel och Tebelius (1987) menar att det finns två ansatser man kan ha när man forskar.

Den första ansatsen är deduktion som enligt Patel och Tebelius (1987) innebär att forskaren tar stöd i teorin för att sedan kunna göra antaganden om hur relationer i verkligheten fungerar. Man kan till exempel titta på hur fåglar förflyttar sig under vinterhalvåret i teorin. Genom denna teori kan man sedan göra ett antagande om varför fåglarna förflyttar sig just då. Detta antagande kan man sedan med testa med hjälp av empiri för att nå ny kunskap. Med andra ord innebär deduktion, ”från teori till slutsats”.

Den andra ansatsen är induktion som innebär att forskaren bygger upp nya teorier utifrån studier av enskilda fall (Patel & Tebelius, 1987). Här kan man till exempel undersöka hur några småföretag har lyckats med en implementation av ett affärssystem. Ur dessa undersökningar försöker forskaren hitta gemensamma drag för att kunna skapa en

allmän teori som gäller för alla småföretag. Induktion betyder alltså, ”från verklighet till teori” och utgår från empirin.

Eftersom det inte existerar mycket information i teorin om digitala signaturer i samband med långsiktigt digitalt bevarande i arkivsystem har vi tänkt använda oss av den induktiva forskningsansatsen.

3.3 Typ av studie

Det finns flera olika sätt att bedriva forskning på. Forskaren kan utforma en undersökning på olika sätt beroende på vilken problemställning som har valts. Tack vare detta kan man klassificera forskningen på olika sätt. Patel och Tebelius (1987) väljer att klassificera olika typer av studier som deskriptiva, explorativa eller hypotesprövande.

Om det inte har forskats mycket inom ett område eller om det finns brister i den forskning som har gjorts inom ett område, väljer man ofta att göra en explorativ studie. I den explorativa studien utforskar man och försöker samla så mycket information som möjligt om ett område för att sedan belysa detta område. Den explorativa studien syftar till att göra ny allmängiltig teori tillgänglig för fortsatta studier. Dessa studier kan också användas för att komma fram till nya forskningsfrågor för framtida studier, som en förundersökning helt enkelt (Patel & Tebelius, 1987).

Om forskaren har tillgång till mycket teori inom ett område och vill kunna förklara varför något ser ut som det gör kan forskaren använda sig av en hypotesprövande studie. Forskaren ställer helt enkelt upp olika hypoteser som sedan provas i verkligheten. Dessa hypoteser ska ha formen av ”om – så” för att forskaren enkelt ska kunna se sambanden mellan olika variabler (Patel & Tebelius, 1987).

Vårt problemområde är relativt nytt och därför finns det inte mycket information att utgå från. Målet med vår studie är dels att belysa ett nytt område, men samtidigt vill vi även utreda hur fortsatt forskning bör bedrivas inom området. På grund av dessa aspekter passar den explorativa studien bäst för vårt område.

3.4 Kvantitativ kontra kvalitativ

När man bedriver forskning kan en studie antingen göras kvantitativ eller kvalitativ. Det ska dock inte ses som svart eller vitt. En kvantitativ studie kan ha kvalitativa drag och tvärtom.

Kvantitativ forskning innebär att statistiska metoder används för bearbetning och analys av det insamlade materialet. Kvantitativ forskning passar sig utmärkt när man gör exempelvis en survey. Kvalitativ forskning innebär att material analyseras verbalt (Patel och Davidsson, 1994).

För att kunna avgöra vilken av metoderna man bör använda i sin forskning kan man titta på vilket det förväntade resultatet av undersökningen blir. Om man vill kunna mäta förekomsten av olika fenomen, beskriva olika relationer mellan dessa fenomen eller förklara hur det ser ut i vår verklighet bör man använda sig av en kvantitativ metod. Däremot om man vill kunna få mer kunskap om dessa relationer, eller förstå varför des-

sa fenomen faktiskt ser ut på ett visst sätt bör man använda sig av en kvalitativ metod (Patel & Tebelius, 1987). För att kunna särskilja kvalitativa undersökningar från kvantitativa undersökningar nämner Bryman (2002) följande grundläggande skillnader:

Kvantitativ	Kvalitativ
* Siffror	* Ord
* Forskarens uppfattning	* Deltagarnas uppfattning
* Teoriprovning	* Teorigenerering
* Strukturerad	* Ostrukturerad
* Hårda data	* Mjuka, fylliga data
* Konstlade miljöer	* Naturliga miljöer

Vårt problemområde och de frågor vi ställer, söker svar på om digitala signaturer är lämpliga för långsiktigt digitalt bevarande. Dessutom vill vi även uppnå en djupare förståelse för problemområdet, vilket kommer att kräva en tolkning av insamlad information från oss som forskare. För att göra detta måste man göra en grundlig analys av materialet, vilket gör att en kvalitativ metod passar bäst för oss.

3.5 Datainsamlingsmetod

Det finns två typer av data man använder sig av i rapporter, primärdata och sekundärdata. Data kan klassas som primär- eller sekundärdata, det är inte bestämt i förväg utan bestäms av vem som samlat in datan och för vilket syfte den samlats in. Är det forskaren själv som samlat in information är det primärdata, har någon annan samlat in informationen är det sekundärdata (Artsberg, 2003).

Primärdata

Primärdata är data som insamlas för uppsatsens specifika syfte. Data som uppstår med hjälp av en intervju är ett bra exempel på primärdata. I fallet med intervjuer är det ett krav att datan är intervjuobjektets självupplevda information, annars kan datan inte klassas som primärdata utan blir sekundärdata istället (Artsberg, 2003).

Sekundärdata

Sekundärdata är redan befintlig data som samlats in i ett annat syfte än för syftet med just undersökningen datan används till. Denna data används för att öka kunskap och medvetenheten inom området (Jacobsen, 2002).

I vår uppsats kommer vi samla in primärdata genom intervjuer samt sekundärdata genom att läsa böcker inom området samt söka vetenskapliga artiklar på olika databaser på internet.

3.5.1 Intervjuer

Bryman (2002) menar att det finns några olika sätt att utföra intervjuer på. Han nämner både ostrukturerade intervjuer och semi-strukturerade intervjuer.

När forskaren utför en ostrukturerad intervju brukar det vara aktuellt att ha skrivit ner några stödord för att kunna sedan kunna låta intervjun flyta iväg efter vad undersökningsobjektet anser vara relevanta frågor att diskutera. Enligt Bryman (2002) tar den ostrukturerade intervjun ofta skepnaden av ett vanligt samtal. Det är också viktigt att den ostrukturerade intervjun är flexibel och att forskaren har möjlighet att ställa följd-

frågor vid behov. Ämnena som avhandlas behöver inte komma i samma ordning som de punkter man har ställt upp bara de avhandlas någon gång under intervjun.

Till skillnad mot en ostrukturerad intervju så ger en semi-strukturerad intervju forskaren möjlighet att styra intervjun litegrann. Ofta har forskaren tillgång till en intervjuguide där vilka teman som ska avhandlas står uppställda. Ibland kan forskaren ha frågor om olika saker i intervjuguiden, men dessa får inte vara för specifika (Bryman, 2002). Ämnena som avhandlas bör komma i samma ordning som i intervjuguiden.

Vi ska använda oss av semi-strukturerade intervjuer i vår studie eftersom vi vill ha tillgång till en intervjuguide och även för att vi vill kunna styra intervjun lite. Eftersom vi undersöker ett väldigt litet och relativt okänt område är det lättare för oss som forskare att kunna styra undersökningsobjekten in på de ämnen vi vill avhandla. Dessutom tror vi att det ger mer struktur till vår intervju genom att ha planerat frågor och teman i förväg.

3.5.2 Intervjuguide

En intervjuguide är bra att ha när man utför intervjuer. Intervjuguiden innehåller ämnen eller punkter som bör avhandlas under intervjun. Bryman (2002) ställer upp några råd för att designa en bra intervjuguide:

- Skapa en ordning bland teman för att få en röd tråd
- Formulera frågor och teman så tydligt som möjligt för att svara på frågeställningen
- Enkelt språk
- Inga ledande frågor
- Ta reda på mycket bakgrundsfakta

Vi har tänkt göra en intervjuguide innan våra intervjuer för att lättare kunna avhandla de ämnen som behövs för att svara på vår frågeställning. För att komma fram till vilka frågor vi ska ställa till respondenterna kommer vi att jämföra problemdiskussionen med den teori vi har valt. Utifrån detta kan vi dra slutsatser om vilka frågor som kommer behövas för att svara på våra forskningsfrågor. För att säkerställa att vi får svar på de frågor vi vill har vi tänkt kontakta forskare inom området för att få feedback på de teman och punkter vi har tänkt ha med i intervjuguiden.

3.6 Urval av respondenter

Vi kommer att vända oss till olika arkiv med vår intervju. Motiveringen till detta är att dessa troligen har praktisk erfarenhet av långtidsbevaring av både digital och icke digital information. På grund av detta bör de ha en uppfattning om vilka problem som finns i dagsläget samt eventuellt förslag på vad som kan göras åt dem. De personer vi kommer att intervjua har vi kommit fram till genom tips från forskare inom detta område. De har tipsat om personer som de tror har den kunskap som krävs för att svara på våra frågor. Vi har även valt intervjuobjekt med olika specialkunskap, övergripande eller tekniska detaljer. Vi har även övervägt att göra en ren litteraturstudie men vi tror att vi kommer få mer och bättre data av personer som sysslar med långtidsbevarande dagligen.

3.7 Analyismetod

Det empiriska material vi får in kommer att analyseras genom att vi kommer att kategorisera den efter de forskningsfrågor vi vill ha svar på. Vi kommer sedan att relatera den till vår teoretiska referensram och med hjälp av våra egna tankar och vår egen tolkning av svaren kommer vi sedan kunna dra slutsatser från den insamlade informationen.

3.8 Validitet och reliabilitet

Validitet

Om validiteten är hög innebär det att en uppsats verkligen mäter eller beskriver det man vill att den ska mäta eller beskriva. Detta gäller främst för en kvantitativ metod. För en kvalitativ metod handlar validitet dessutom om resultatet av datainsamlingen tolkas på ett bra sätt (Jensen, 1995).

I vårt arbete försöker vi höja validiteten på följande sätt:

- Intervjuguide – Genom att använda oss av en intervjuguide säkerställer vi att de frågor vi behöver för att svara på vår frågeställning kommer att ställas.
- Intervjuobjekt – Vi kommer att intervjua personer med både praktisk och teoretisk erfarenhet inom området för att få så bra data som möjligt inför analysen.
- ~~Frågor~~ Frågor. Vi kommer även försöka formulera flera frågor som svarar på samma sak fast på olika sätt för att minska risken att intervjuobjektet missuppfattar frågan, och därmed ger ”rätt” svar.
- Externa synpunkter – När vi utformat vår intervjuguide kommer vi att göra en pilot-intervju med någon utomstående för att säkerställa att vi inte missar att ställa någon viktig fråga. Denna utomstående ska givetvis vara insatt inom området långsiktigt digitalt bevarande och digitala signaturer.
- Inspelning – Vi kommer att spela in intervjuerna på band för att kunna återskapa datan. Syftet med detta är att vi ska kunna gå tillbaka och lyssna på svaren igen vid oklarheter.

Reliabilitet

Om reliabiliteten är hög innebär det att en undersökning skulle ge samma resultat vid olika tillfällen under samma förutsättningar. Detta gäller främst för en kvantitativ metod. För en kvalitativ metod handlar reliabilitet snarare om precisionen av resultatet. Med precision menas hur oberoende resultatet är av yttre faktorer. Reliabilitet i kvalitativa undersökningar handlar även om hur resultatet påverkas av omständigheter som forskaren inte kan kontrollera. Ett lägre antal yttre faktorer ger högre reliabilitet (Jensen, 1995).

För att höja reliabiliteten i våra intervjuer har vi valt att skicka intervjumaterialet efter sammanställning till intervjuobjekten. I och med det har våra respondenter fått chansen att godkänna eller ändra materialet. På grund av detta borde likadana studier ge liknande resultat om någon annan genomför dem.

4. Empiri

I detta kapitel presenteras resultatet av våra intervjuer. Vi kommer att presentera informationen efter de forskningsfrågor vi vill ha svar på. Vi presenterar de resultat vi anser vara relevant.

4.1 Intervju med Göran Kristiansson på Riksarkivet

Göran är chef för samordnings och utvecklingsenheten på Riksarkivet vilket innebär att han har arbetat med området.

4.1.1 Digitala signaturer i arkivsystem

När vi talar om digitala signaturer som en teknik för att lösa autenticitetsproblem på lång sikt menar Göran att kryptering med checksummor är väldigt bra att använda. För att exemplifiera detta tar han skatteverket som ett exempel. Han berättar att när skatteverket tar emot en deklaration används en publik nyckel för att kunna identifiera upphovsmannen till deklarationen. Han anser att denna form av digitala signaturer är väldigt bra för att identifiera upphovsmannen till en digital handling samt för att kunna säkerställa att informationen är oförändrad. Han menar att tankarna förs tillbaka i tiden till de sigill som användes då. När vi frågar Göran om vattenmärkning som ett alternativ till kryptering anser han att det är bra för att skydda copyright, alltså för att säkra handlingen, men han säger att han samtidigt tror att det förmodligen är lättare att kontrollera om en checksumma är giltigt än att kontrollera att ett vattenmärke är giltigt. Göran säger att han inte har arbetat med vattenmärkning särskilt mycket, men tycker trots detta att vattenmärkning kan vara ett tänkbart alternativ till kryptering. Om man bortser från att handlingen förändras genom vattenmärkning och därmed inte är en legal handling tycker Göran att autenticiteten bara skulle förstärkas med vattenmärkning i kombination med andra digitala signaturer.

Göran anser att olika krypteringssystem i arkivsammanhang är enkla att införa eftersom det är en ganska väletablerad teknik. Han förtydligar sedan med att säga att det förmodligen inte alltid är lätt att införa, men att det är nödvändigt för att människor ska kunna känna sig trygga med transaktioner på Internet och för att människor ska kunna lita på digitala handlingar. Allting handlar dock inte om hur enkelt det är att införa menar Göran, kostnadsfrågor spelar givetvis en roll. Tyvärr har inte Göran någon uppfattning om hur mycket det kostar att införa krypteringssystem för arkiven, men han anser att det är väldigt enkelt att använda systemen när dessa väl är på plats. ”Jag har själv aldrig haft några problem med att installera, stämpla och skicka handlingar. Fast jag kanske inte är representativ för allmänheten eftersom jag ofta använder en dator.”

4.1.2 Digitala signaturer i samband med långsiktigt digitalt bevarande

På frågan om vilka problem som finns med digitala signaturer i kombination med digitalt bevarande svarar Göran att riksarkivet har diskuterat denna fråga. Han berättar att det arkivinformatonssystem som riksarkivet hanterar idag kan ses som en sökingång till alla arkiv som finns i landet. I den nationella arkivdatabasen ska riksarkivet lagra allting som kommer in till deras system. Frågor som har dykt upp på riksarkivet enligt Göran är bland annat hur de ska gå tillväga för att lagra alla dessa digitala handlingar.

Som ett exempel nämner han att både försäkringskassan och skatteverket skickar in deras digitala handlingar till Riksarkivets system. Eftersom det handlar om cirka 80000 ärenden per dag bara på försäkringskassan är det ju ett enormt arbete att kontrollera äktheten i deras handlingar samt dessa handlingars signaturer. Riksarkivet har kommit fram till att de inte ska kontrollera äktheten i handlingarna eller signaturerna utan de ska istället skapa plats för att visa att signaturen har funnits på handlingen en gång i tiden. Detta innebär att om en privatperson kommer in och ber att få ut en handling, går det att se att informationen i den digitala handlingen har varit oförvanskad sedan den kom in till arkivet.

När det gäller problem på lång sikt nämner Göran att digitala signaturer har en begränsad livslängd. Han tar 5 år som ett exempel. Han funderar sedan över hur man gör om 50 år för att se om man har tillgång till en giltig handling eller en förfalskning? Riksarkivet menar att en säker hantering av informationen, bra rutiner och bra dokumentation av vad som händer med informationen leder till att det behovet blir tillgodosett. Han påpekar även att man kan sätta en ny checksumma på en konverterad handling för att även i framtiden kunna påvisa att informationen i den digitala handlingen är oförändrad.

På en direkt fråga om ett sätt att lösa formatbyten är att signera om handlingar och om riksarkivet planerar att utföra dessa åtgärder svarar Göran att de inte kommer att signera om de digitala handlingar de har fått in. Han tror helt enkelt att det är för många handlingar. Vid ett formatbyte kommer de istället att konvertera handlingen rakt av och skapa ett system som ger spårbarhet bakåt i tiden. Det ska helt enkelt finnas information om varje digital handling där det beskrivs hur handlingen har påverkats sedan den kom in till arkivet. Informationen kan innehålla information om till exempel hur en konvertering till ett nytt format har gått till samt om handlingen har blivit omsignerad. Denna information kommer även styrka autenticiteten i framtiden.

Göran påpekar dock att autenticitet och spårbarhet inte alltid är en teknisk fråga utan kan handla om en så enkel sak som att följa ett regelverk. Exempelvis kan detta innebära att man skapar kopior av ett verk och lagrar en kopia i Lund och en kopia i riksarkivets arkiv. Att man helt enkelt har en säker hantering av de digitala handlingarna.

4.1.3 Trusted Archival Services

På frågan om de arkiv som existerar idag är beredda att ta ansvar för digitala handlingars och digitala signaturers autenticitet enligt den modell som presenteras i TAS anser Göran att det isåfall blir en enorm operation, givetvis beroende på vilket arkiv som avses. Han fortsätter med att förklara att det bland annat kan handla om regionala arkiv, kommunarkiv och myndighetsarkiv. På riksarkivet förvaltar de cirka 65000 handlingar idag och att signera om dessa som TAS föreskriver måste tänkas över väldigt noga av arkiven själva anser Göran. Att TAS är ett realistiskt koncept för lite mindre arkiv tvekar han inte på, men för ett arkiv av riksarkivets storlek blir det en större mängd information som måste hanteras. Dock är det egentligen en praktisk fråga enligt Göran. Att arkiven ska presentera en lista med vilka format de tar emot är en bra sak enligt Göran. Han berättar att vi i Sverige kan ställa krav på detta sätt, medan det i många länder utomlands inte alls går att ställa sådana krav, vilket också har lett till att till exempel USA har ett jätteproblem att hantera eftersom de har så många olika format.

Den distribuerade modell som nämns i TAS tror inte Göran är någon bra ide. Han styrker detta med att berätta att han inte tror att riksarkivet har kapacitet att hantera alla handlingar som isåfall skulle ligga ute på andra arkiv. De har diskuterat den iden på riksarkivet tidigare, men kommit fram till att det förmodligen skulle innebära stora informationsförluster eftersom myndigheterna själva är betydligt sämre rustade för lagring samt konvertering till nya format. Han tror att det helt enkelt är bättre att samla alla digitala handlingar på riksarkivet och utföra lagring och konvertering på ett ställe. Både signaturer och handlingar bör alltså lagras på samma plats enligt Göran. Från det Göran vet om TAS tycker han att konceptet låter bra för att eliminera de problem med digitala signaturer i kombination med långsiktigt digitalt bevarande som existerar idag, förutom kravet på att arkiven själva ska signera om de digitala handlingar som finns i deras arkiv. Det är ett realistiskt krav för många arkiv resonerar Göran.

4.2 Intervju med Lars-Erik Hansen på TAM-arkiv

Lars-Erik Hansen är VD på TAM-arkiv som är en ideell förening vars uppdrag är att förvara, vårda, tillgängliggöra och tillhandahålla medlems-organisationernas arkivmaterial. TAM-Arkiv ska också svara för medlemmarnas kompetens-försörjning i alla frågor som gäller den arkivnära informationshanteringen, till exempel framtagning av dokumenthanteringsplaner.

4.2.1 Digitala signaturer i arkivsystem

Enligt Lars-Erik är syftet med kryptering med hash-summor att mottagaren ska kunna säkerställa vem upphovsmannen till en digital handling är samt att verifiera att informationen är oförändrad. Lars-Erik anser alltså att kryptering med checksummor erbjuder hög identitet och integritet. På frågan om vattemärkning svarar Lars-Erik att han inte arbetat med det tidigare och alltså inte har någon uppfattning om detta.

Att införa ett krypteringssystem i arkivsammanhang anser Lars-Erik vara ganska svårt. Det är mycket man måste tänka på innan man inför systemet. På försäkringskassan där han arbetade tidigare var det inte prioritet på att kunna garantera handlingarnas säkerhet på sikt. Lars-Erik påpekar också att det är väldigt viktigt att checksummor måste kontrolleras vid ankomst till arkivet. Om ny information om en handling kommer in till arkivet måste arkivet även jämföra denna information med handlingen för att se om informationen är relevant. Att använda krypteringssystemen är även det väldigt enkelt enligt Lars-Erik. Handläggarna märker oftast inte vad som sker i det bakomliggande systemet. På försäkringskassan där Lars-Erik tidigare arbetade skedde krypteringen per automatik och Lars-Erik tycker att det var enkelt att använda det. Däremot har Lars-Erik ingen uppfattning om kostnader när det gäller att införa dessa system. Han har inte själv varit med vid upphandlingarna av systemen.

4.2.2 Digitala signaturer i samband med långsiktigt digitalt bevarande

De problem som uppstår vid långsiktigt digitalt bevarande är flera enligt Lars-Erik. Han nämner följande problem:

Ju längre tiden går desto osäkrare blir den digitala signaturen, vilket beror på olika faktorer. Dessa faktorer kan vara att handlingen byter format, att nyckel-certifikat inte fungerar tillfredsställande samt att algoritmer knäcks. Lars-Erik anser vidare att ett annat

stort problem är att det är enormt svårt att skapa spårbarhet lång tillbaka i tiden. En möjlig lösning för att säkra certifikat nämner Lars-Erik är att signera om de digitala handlingarna med jämna mellanrum, men han nämner även att man bör ha en säker hantering vid lagringen. För att arkiven ska bli betrodda diskuteras det om man ska använda sig av såkallade tredjeparts betrodda aktörer där man lagrar kopior på två ställen. Ett sätt att lösa detta finns i OAIS-modellen där de föreslår att arkivet skickar ut en kopia och att arkivet själva alltid har kvar originalhandling. På detta sätt är säkerheten delvis inbyggd men alla rutiner för säker hantering måste också följas.

För att höja autenticiteten bland digitala handlingar säger Lars-Erik att man kan tänka på vad som gjorts i pappersvärlden. Där har man använt sig av Proginens, vilket innebär att information ska ses i sitt sammanhang för att man ska kunna avgöra om den är äkta. Man måste ha stor kunskap inom ett område för att kunna manipulera något och för att det ska verka trovärdigt. För att göra en sammanhangskontroll förutsätter det att man följer de processer som handlingen har verkat i. Som ett exempel nämner Lars-Erik att om man finner ett dokument om ekonomistyrning som har framkommit i en systemutvecklingsprocess är det mest troligt att dokumentet är förfalskat eftersom det inte passar i sammanhanget. Autenticitet består inte bara av digitala signaturer utan även av proginens. Ett annat sätt att höja säkerheten på är att utforma åtkomsten så att den inte möjliggör manipulation säger Lars-Erik.

4.2.3 Trusted Archival Services

Det är väldigt realistiskt att använda sig av TAS om man förenklar signeringstekniken enligt Lars-Erik. Omsigeringen bör inte bygga på gamla signaturer utan istället bygga på arkivets nya signatur för handlingen. Man måste även ta hänsyn till vad som ska signeras. Det kan vara aktuellt att signera loggar över hur handlingar har förändrats över tiden. Lars-Erik menar att det är viktigt att minimera antalet åtgärder vid hantering av handlingarna för att minska arbetsbördan för arkiven. Detta bland annat på grund av det stora antalet handlingar som kan finnas i ett arkiv. Arkiven bör inte heller bevara allting, det blir för mycket information i längden. En tänkbar handling att lagra är loggar över hur handlingarna har påverkats. Istället för att granska alla detaljer i till exempel en bok kan man enkelt granska loggen över vad som hänt med handlingen genom åren och därigenom dra slutsatser om dess äkthet.

På frågan om vad Lars-Erik anser om den distribuerade modell som TAS föreslår anser han att det blir stora problem för myndigheter att hålla reda på sina certifikat, vilken information som lagras samt vilka algoritmer som används för signaturer. Det blir helt enkelt för mycket information att hålla reda på.

Men för att arkiven själva ska börja följa TAS eller något liknande koncept anser Lars-Erik att detta är en fråga för arkivmyndigheten som måste skapa riktlinjer för arkiven att följa. Han tror att inget arkiv i grund och botten vill lida av informationsförluster. Problemet som han ser det idag är att det är svårt att motivera ledningen av arkiven. För att motivera ledningen är det väldigt viktigt att kunna ta upp frågor som varför de ska ha lösningen och vilken vinst detta genererar. Kan man påvisa dessa vinster samt att arkivmyndigheten utformar riktlinjer att följa är det givetvis mer troligt att arkiven tar ansvar för digitala handlingar äkthet och autenticitet.

Slutligen säger Lars-Erik att TAS inte är någon slutgiltig lösning, men han anser att TAS är en bra början för att lösa de problem som uppstår vid långtidsbevarande av digitala handlingar. Dessutom menar han att bättre lösningar kommer att utvecklas ju längre tiden går. I dagsläget anser han att det är viktigt att behandla frågor som till exempel vilka format som ska hanteras, om omsigtering bör utföras samt andra faktorer.

4.3 Intervju med Magnus Wählberg på Skatteverket

Magnus Wählberg är arkivarie med erfarenhet som specialist inom digital dokumenthantering. Han har även arbetat med frågor om formathantering inom Försäkringskassan. Idag arbetar han som arkivarie på Skatteverket.

4.3.1 Digitala signaturer i arkivsystem

Magnus anser att kryptering med hash-summor kan garantera en handlingens integritet och identitet under en tidsperiod på 5-10 år. Efter den tiden är den digitala signaturen oftast värdelös, vilket gör att det blir svårt att garantera den digitala handlingens identitet och integritet. Magnus anser även att vattenmärkning kan vara bra för detta ändamål, dock ser han inte hur integriteten ska kunna garanteras eftersom det inte finns någon spårbarhet om vattenmärket skulle förändras.

På frågan om det är enkelt att införa ett krypteringssystem tycker Magnus att det är väldigt enkelt på kort sikt. När man ska införa ett system som ska kunna hantera digitala handlingar på lång sikt anser han att det är svårt på grund av att det finns många faktorer att ta hänsyn till. Idag känner han inte till någon som har ett system för att kunna upprätthålla signaturer på lång sikt. Vad gäller kostnadseffektiviteten anser Magnus att man ska jämföra lagring av digitala handlingar med lagring av pappershandlingar för att kunna avgöra kostnadseffektiviteten. Lagring av pappershandlingar kräver mycket manuellt arbete som kostar mycket. Vid små volymer anser Magnus att krypteringssystemen inte är kostnadseffektiva. Däremot anser han att investeringskostnaden för ett krypteringssystem är mindre än kostnaden för att hantera pappershandlingar manuellt. Att det är enkelt att använda finns det ingen tvekan på menar Magnus. Det mesta sker ju per automatik, till exempel omsigtering.

4.3.2 Digitala signaturer i samband med långsiktigt digitalt bevarande

Magnus anser att det är ett jätteproblem med digitala signaturer i samband med långsiktigt digitalt bevarande. De problem på lång sikt som Magnus kan se är att certifikatshandlingen är dålig, att signaturen har knäckts, att nyckellängden är för kort samt att produktleverantörer av krypteringssystem inte har support för sina system längre. Digitala signaturer används för att knyta en person till en handling samt för att kunna garantera handlingens integritet. Detta gör att det även är svårt att bygga upp en bra infrastruktur för att kunna använda digitala signaturer för lagring av digitala handlingar.

Idag finns det några olika alternativ för hantering av digitala handlingar. Magnus säger att ett alternativ är att man kan ta emot en handling och dess signatur i ett ankomstregister och lagra dessa i ett paket. Detta paket kan man sedan gå tillbaka till för att se hur handlingen och dess signatur såg ut när de kom in till arkivet. Ett annat alternativ enligt honom är parallell lagring, vilket innebär att man lagrar en kopia på ett annat ställe. Ett

tredje alternativ är att arkivet själv signerar om den digitala handlingen med arkivets egna signatur. Detta innebär att man behöver en säker process för omsignering. Vid konvertering blir det oftast problem att signera om en handling. Ett problem är att upphovsmannen till en handling inte är delaktig i denna process, alltså tappar man lite av autenticiteten eftersom man måste lita på arkivets signeringsprocess. Man tappar helt enkelt kopplingen mellan personen och handlingen. Det handlar också om kostnaden vid införande av en säker process.

För att lösa dessa problem har det diskuterats om att ha en tredje part som är betrodd vilken ska signera om handlingar och tidsstämpla dessa. Tankar om att införa en sådan tjänst i Sverige finns idag, men än så länge finns det ingen som gjort det. Magnus anser att en central tjänst som garanterar tillsammans med en säker process för hanteringen av digitala handlingar och dess signaturer gör att man kan garantera äktheten i en handling utan att upphovsmannen är delaktig.

Magnus anser dock att det inte finns någon generell lösning idag för att garantera en handlingens autenticitet. Det är helt enkelt för många parametrar att ta hänsyn till. Förutom de sociala aspekterna måste man ta hänsyn till de tekniska samt juridiska aspekterna.

4.3.3 Trusted Archival Services

Magnus anser att TAS är ett bra koncept för att hantera digitala handlingar och dess signaturer på lång sikt. Dock tror han att risken finns att det bara blir en papperstiger. Att arkiven är beredda att införa detta är han dock inte säker på. Han anser att detta är en kostnadsfråga. För att arkiven ska kunna införa TAS måste man kunna motivera ledningen. Oftast säger ledningen ja till själva omsigneringen, men inte till hela lagringsprocessen. Alltså kan vissa saker som exempelvis spårbarhet och verifiering utebli.

Kraven som ställs på ett arkiv i TAS är bra enligt Magnus, men det kommer ändå att bli problem med formatbyten om 20-30 år. Man skjuter alltså bara problemet framför sig. Även här måste man tänka på investeringskostnaden för att se om det är ett realistiskt koncept för sin organisation.

De problem som digitala signaturer har på lång sikt löser TAS delvis. Bland annat försvinner äkthetsproblemet eftersom man får ett betrott arkiv som hanterar alla handlingar. Att kunna visa på kopplingen mellan person och handlingar kvarstår dock som ett problem. Magnus anser också att flera olika format är väldigt krångligt att hantera i praktiken. Därför tycker han att det vore bra om man kunde hålla sig till ett standardformat. Detta standardformat skulle till exempel regeringen kunna fastställa. Man skulle till exempel kunna använda sig av XML som format. Han menar att detta inte bara blir lättare utan även ger en kostnadsmässig fördel för arkiven eftersom man inte behöver hantera flera olika format. Däremot kanske inte alla leverantörer tycker om att behöva anpassa sina produkter efter ett format.

5. Analys och Diskussion

I vår analys och diskussion kommer vi knyta vår teoretiska referensram mot det empiriska material vi har samlat in. Vi för även en diskussion som leder mot svaret på våra forskningsfrågor.

5.1 Digitala signaturer i arkivsystem

Enligt RLG och OCLCs rapport, ”*Trusted Digital Repositories: Attributes and Responsibilities*” är det väldigt viktigt för digitala arkiv att hantera frågor om handlingarnas identitet och integritet. Detta är de faktorer som leder till att autenticiteten hos en digital handling är hög. Med hög autenticitet är chansen större att slutanvändarna kan lita på äktheten i en digital handling i framtiden. Att autenticiteten hos digitala handlingar bör vara så hög som möjligt anser vi vara självklart. På lång sikt vill man kunna lita på att informationen är korrekt, men även att upphovsmannen är den man tror. Vi tror att det är väldigt viktigt för arkiven att införa system för digitala signaturer för att höja autenticiteten.

För att kunna garantera att en handling har hög autenticitet har man lånat tekniken med digitala signaturer från området elektronisk handel (Lynch, 1999). Två typer av digitala signaturer är kryptering med checksummor och vattenmärkning vilka båda enligt teorin kan användas till att identifiera en upphovsman samt att verifiera att informationen i en digital handling är oförändrad. Två av respondenterna ansåg att kryptering med checksummor är en bra teknik för att säkerställa en digital handlingens upphovsman och att informationen i handlingen är oförändrad. En respondent menar dock att kryptering med checksummor bara är giltig på kort sikt. Denna respondent talar om 5-10 år som ett exempel, efter denna tid anser han att den digitala signaturen är värdelös. Detta gör att identiteten och integriteten inte kan garanteras på lång sikt.

På frågan om vattenmärkning svarade en respondent att han inte ville uttala sig för att han inte hade någon uppfattning om området i sig. En annan respondent tyckte att vattenmärkning verkade vara en bra teknik för detta skäl om man använder det i kombination med kryptering, men han påpekade även att han inte hade någon större erfarenhet av vattenmärkning sedan tidigare. Den sista respondenten tror dock att integriteten blir svår att garantera vid ett senare skede eftersom han inte kunde se hur spårbarheten realiserar med vattenmärkning. Här anser däremot Wickström (2004) att digital vattenmärkning hanterar just denna fråga. Genom att vattenmärket förstörs om den digitala handlingen förändras, hålls integriteten hos den digitala handlingen på en fortsatt hög nivå.

Enligt oss verkar både vattenmärkning och kryptering med checksummor vara giltiga tekniker för detta ändamål på kort sikt, vilket också en respondent svarade. Dumortier och Van den Eynde (2005) visar också att digitala signaturer har problem på lång sikt eftersom signaturerna kan knäckas. Vi anser dock att detta är en väldigt bra början. Vi anser att nya, mer effektiva tekniker bör utvecklas som både gör att de digitala signaturerna blir svårare att knäcka samt att de blir lättare att hantera. Vi tror att man genom detta förmodligen har större chans att upprätthålla de digitala handlingarnas autenticitet. I dagsläget tycker vi att det låter utmärkt att kombinera kryptering med vattenmärkning för att få en högre grad av autenticitet på de digitala handlingarna på kort sikt.

Frågan om att införa dessa system i praktiken möttes av blandade svar. En respondent ansåg att det var enkelt att införa eftersom det handlar om en väletablerad teknik. En annan respondent ansåg tvärtom att det var svårt att införa på grund av alla faktorer man måste ta hänsyn till. Denna respondent menar att arkivet måste ta ställning till vad de ska hantera, hur länge man ska lagra det och vilken säkerhet de vill ha och att det därför inte alltid är enkelt att införa. Den tredje respondenten svarade att det är lätt att införa ett krypteringssystem på kort sikt. Däremot tycker han, liksom en annan respondent tidigare nämnt, att det är väldigt många faktorer att ta hänsyn till för ett införande som ska fungera på lång sikt. Detta visas även på av Morisio et. Al (2002) som menar att det finns flera problem som kan uppstå vid införande av ett system i en organisation. Vi tror att skälet till att vi fick fram blandade åsikter om hur enkelt det är att införa ett sånt här system beror på att respondenterna arbetar på olika arkiv, vilka har olika syften. Till exempel arbetar en av respondenterna på riksarkivet, där man måste lagra all information som kommer in i arkivet. På TAM-arkivet arbetar en annan respondent, där har de friheten att välja vad de vill lagra och ställs då inför frågan om vad man vill lagra och hur länge med vilken säkerhet. Vår personliga åsikt är att det oftast är enkelt att införa ett sånt här system eftersom det är en väletablerad teknik. Vi tror också att man, precis som flera av våra respondenter svarade, måste ta hänsyn till flera faktorer vid lagring på lång sikt.

Endast en respondent hade någon uppfattning om kostnadsfrågor för införande av ett krypteringssystem. Denna respondent ansåg att man måste jämföra kostnaden för ett digitalt system med ett system som hanterar pappershandlingar. Han ansåg att ett digitalt arkiv som hanterar många handlingar blir mer kostnadseffektivt än ett som hanterar få. När det är frågan om få handlingar tror en respondent att pappershandlingar är ett bättre alternativ. En annan respondent ansåg att kostnaden var en viktig fråga att ta hänsyn till eftersom det oftast är den som avgör om arkiven ska investera i ett system för digitala signaturer. Vi tror att det är dyrt att införa ett system för digitala signaturer eftersom dessa system oftast skräddarsys mot den verksamhet eller det arkiv som det ska verka i. Sundgren (2003) visar dock att det generellt sett är mindre kostsamt att använda standardsystem än att utveckla nya system från grunden. Vi håller även med den respondent som svarade att det gäller att göra en avvägning mellan pappershantering, digital hantering samt mängden handlingar som ska hanteras.

Två av våra respondenter ansåg att kryptering med checksummor är en väldigt enkel teknik att använda sig av. De har inte märkt av den underliggande tekniken när de har använt sig av dessa typer av system. Den tredje respondenten menade däremot att det var väldigt enkelt att använda dessa system då det mesta kan ske per automatik. Vi båda anser att det är väldigt enkelt att använda krypteringssystem eftersom vi har provat på det båda två. Att det är enkelt bekräftas även av Axelsson, Fihn, Rosenqvist (2003) som menar att dagens system för digitala signaturer är väldigt enkla att använda. De visar att systemen sköter autenticeringen av de digitala handlingarna per automatik.

5.2 Digitala signaturer i samband med långsiktigt digitalt bevarande

Enligt två respondenter finns det flera problem på lång sikt med att använda digitala signaturer för att höja autenticiteten hos digitala handlingar, vilket stöds av Lynch (1999). De problem som identifieras i teorin är följande:

- Formatbyten
- Ny teknik
- Begränsad livslängd på signaturen
- Upphovsmannen finns inte tillgänglig
- Tillit till tredje part

Två av respondenterna konstaterar att formatbyten är ett problem. Att ny teknik utvecklas är ett underförstått problem eftersom det är det som leder till att arkiven kommer att bli tvingade att byta format på sina digitala handlingar på lång sikt. Alla respondenter nämner att begränsad livslängd på de digitala signaturerna är ett stort problem. En respondent menar att nyckellängden på den digitala signaturen kan vara för kort, att algoritmen kan knäckas samt att produktleverantörer inte har support för sina produkter i framtiden. Eftersom det utvecklas ny teknik hela tiden tror vi att det blir lättare att knäcka de algoritmer som används för kryptering idag.

En av respondenterna menar att en säker hantering av informationen, bra rutiner och bra dokumentation kring de digitala handlingarna leder till att arkiven kan hantera problemen med digitala signaturer bättre. Vi anser att det är självklart att detta är viktiga frågor att ta ställning till. En säker hantering av de digitala handlingarna leder ju i slutändan till att autenticiteten höjs. Ett annat alternativ för att motverka de digitala signaturernas problem enligt alla respondenter är att arkiven får signera om de digitala handlingarna. En respondent tror dock att detta blir en enorm operation för arkiven och att det inte är realistiskt. Vi håller inte med om detta. Att signera om digitala handlingar är en operation som för det mesta sker per automatik, vilket stöds av två respondenter. Vi tror också att autenticiteten höjs när omsigneringen sköts automatiskt eftersom det minskar risken för mänskliga fel. Däremot tror vi att det kan bli stora problem vid formatbyten om arkiven har många digitala handlingar att signera om. Eftersom arkiven i det fallet måste kontrollera handlingarna manuellt och inte per automatik för att se om dessa är godkända bör det vara en väldigt tidskrävande operation, ett problem som även nämns av en respondent. Samma respondent ser även att ett problem kan vara att upphovsmannen inte längre är tillgänglig vid omsigneringen. I detta fall anser han att man tappar kopplingen mellan person och handling eftersom man måste lita på arkivets signatur och dess process.

En respondent anser att spårbarhet är en viktig fråga för arkiven. Denna respondent menar att man bör lagra ett dokument som visar hur varje digital handling har förändrats över tiden. En annan respondent håller med om att loggar är en bra metod för detta, men säger samtidigt att det är enormt svårt att skapa en fungerande spårbarhet långt fram i tiden. Den tredje respondenten menar att arkiven kan lagra alla digitala handlingar som kommer in tillsammans med deras digitala signaturer i ett paket. Detta paket kan man sedan gå tillbaka till och undersöka för att se hur handlingen såg ut när den kom in till det digitala arkivet. Själva idén med spårbarhet är väldigt bra tycker vi. Vi tror dessutom att det inte är något problem på lång sikt. Att förutom att tillhandahålla

en säker hantering av de digitala handlingarna erbjuda spårbarhet bakåt i tiden höjer snarare autenticiteten i våra ögon om arkiven är certifierade.

Andra problem som avhandlas i teorin är om upphovsmannen fortfarande finns tillgänglig eller om tilliten till tredje part brister (Lekkas & Gritzalis, 2004).

Dessa problem pekar även en av våra respondenter på och föreslår att man bör använda sig av såkallade tredjeparts betrodda aktörer som certifierar de digitala arkiven i framtiden för att motverka att tilliten till tredje part brister. På det viset blir man betrodd som ett digitalt arkiv. Vi tycker att detta låter som en utmärkt ide. I framtiden hade vi gärna kunnat gå till exempelvis en myndighet för att se vilka digitala arkiv som är certifierade, det vill säga betrodda. En respondent har en lite annorlunda lösning på detta problem. Denna respondent menar att det bör finnas en betrodd tredje part, men istället för att certifiera arkiven bör dessa aktörer signera och tidsstämpla handlingar. Om dessa aktörer kan visa att de har en säker process för signering och tidsstämpling kan man garantera autenticiteten i de digitala handlingarna utan att upphovsmannen är inblandad.

För att ytterligare höja autenticiteten i ett digitalt arkiv säger en respondent att man bör tillämpa en kontroll på vilket sammanhang handlingen har skapats inom för att kunna avgöra om handlingen är äkta. För att kunna göra detta bör arkiven titta på vilka processer som har genererat den digitala handlingen. Vi tror att detta är ett bra komplement till de tekniker som finns om det finns oklarheter om de digitala handlingarnas äkthet. Att utföra denna kontroll som är väldigt resurskrävande för varje handling man får in är väldigt onödigt utan bör endast utföras om något ifrågasätts.

En annan respondent nämner att ytterligare ett sätt att upprätthålla autenticiteten hos digitala handlingar är parallell lagring. Detta innebär att man lagrar en kopia av den digitala handlingen på ett annat säkert ställe. Om en handling förstörs på något sätt finns alltid en kopia av originalhandlingens kvar.

Som visats finns det flera problem med digitala signaturer när man behandlar långsiktigt digitalt bevarande. Flera olika lösningar på de olika problemen har framkommit, men i grund och botten anser vi att digitala signaturer är en kortsiktig lösning.

5.3 Trusted Archival Services

TAS är ett koncept som tagits fram av EESSI för digitala arkiv. Konceptet ska garantera att digitala handlingar ska kunna bevaras på lång sikt med hög autenticitet. Detta koncept riktar sig mot arkivvärlden. För att kunna nå målet ställs fyra krav på ett arkiv, handlingarnas format, teknologisk interoperabilitet, bakåtkompatibilitet samt kryptografisk uppföljning (EESSI, 2000).

Att införa detta koncept innebär ju arbete för arkiven men en respondent anser att kraven som ställs på ett arkiv i TAS är väldigt realistiska, medan en annan respondent anser att den kryptografiska uppföljningen innebär för mycket arbete för arkiven. Denna respondent kan däremot se att konceptet passar utmärkt för mindre arkiv. Den sista respondenten anser att kraven är bra, men påpekar samtidigt att omsigeringen vid formatbyten kommer vara ett problem. Han menar att man bara skjuter problemet framför sig.

För att minska bördan på det arkiv som vill införa TAS anser en respondent att man bör förenkla tekniken för att signera om de digitala handlingarna. Denna respondent tycker att arkiven själva borde ha en egen signatur som de signerar om handlingarna med, vilket skulle underlätta eftersom arkiven inte skulle behöva hålla reda på olika signaturer för olika handlingar. En annan tanke som denna respondent hade var att arkiven inte bör lagra allting eftersom att det blir för mycket information i längden. En annan respondent nämner dock att i vissa organisationer ska all information lagras. Vi tror att TAS är ett realistiskt koncept. Skälet som en respondent anger vara en nackdel tycker inte vi är något problem. Omsigneringen sköts ju oftast per automatik enligt de andra två respondenterna. Dock kan det bli mycket arbete just vid formatbyten eftersom handlingarna måste kontrolleras manuellt.

Vad gäller den distribuerade modellen anser två respondenter att den är mindre bra, den kommer leda till informationsförluster eftersom till exempel myndigheter redan idag är sämre rustade att lagra sina handlingar i jämförelse med de arkiv som bara sysslar med bevaring. En av dessa respondenter menar också att riksarkivet inte har kapacitet att hantera signaturer för alla handlingar som olika myndigheter kan tänkas spara. Att dessutom behöva lagra information om vilka signaturer som tillhör vilka handlingar blir svårt. Både signaturer och handlingar bör alltså lagras på samma plats enligt en respondent. Vi tror inte heller på den distribuerade modellen som EESSI föreslår inom långsiktigt digitalt bevarande. Det kan bli svårt för arkiven, om inte omöjligt, att ta ansvar för att handlingar har hög autenticitet om man bara lagrar signaturer på arkiven. Den centraliserade modellen där man lagrar både handlingar och signaturer på arkiven är att föredra.

För att få arkiven att införa TAS anser en respondent att arkivmyndigheten bör skapa riktlinjer för arkiven att följa. Problemet som han ser det idag är att det är svårt att motivera ledningen av arkiven att förändra organisationen så att de följer dessa krav. En annan respondent är också inne på samma tankegångar angående motivering av ledning. Denna respondent menar att ledningen oftast går med på själva omsigneringsprocessen, men inte till hela lagringsprocessen. Vi ser också att detta kan vara ett problem för arkiven. Det finns mycket litteratur inom området Systemvetenskap som visar på problematik med förändringar i organisationer. Skulle man däremot kunna visa på de vinster som arkiven gör med detta koncept så känner vi att ledningen skulle vara mer motiverade till införande av konceptet. I grund och botten tror vi att arkiven vill vara så robusta som möjligt och ha möjlighet att lagra handlingar på lång sikt med hög autenticitet.

Alla respondenter tror att TAS kan eliminera de problem som existerar idag med digitala signaturer inom långsiktigt digitalt bevarande. De krav som ställs på ett arkiv som vill bli ett TAS eliminerar de flesta problem som existerar med digitala signaturer idag. En respondent säger att även äkthetsproblemet försvinner med hjälp av TAS eftersom man får ett betrott arkiv som hanterar alla handlingar. Samma respondent skulle gärna vilja se en förändring på vilka format arkiven ska stödja. Han skulle föredra ett enda format som blir standard, detta skulle leda till en kostnadsfattig och administrativ fördel. Vi tror starkt på detta förslag, att bara behöva hantera ett format borde underlätta väldigt mycket för arkiven. I övrigt nämner en annan respondent att han ofta har tänkt och förespråkat nästan samma sak som TAS, han ser därför väldigt positivt på TAS som koncept.

6. Avslutning

I vår studie har vi försökt nå ny kunskap om digitala signaturer och dess användande inom långsiktigt digitalt bevarande. Det finns många frågor på detta område som bör behandlas av vilka vi har valt att börja med de grundläggande. Efter att ha presenterat slutsatser på våra forskningsfrågor avslutar vi med att knyta samman forskningsfrågorna till en övergripande bild av området. Detta kapitel avslutas med en metoddiskussion där vi diskuterar de val vi har gjort vid genomförandet av studien.

6.1 Slutsatser

6.1.1 Digitala signaturer – en lämplig teknik?

Slutsatsen vi kan dra av denna studie är att digitala signaturer inte är en lämplig teknik för att säkerställa autenticiteten i digitala handlingar på lång sikt. På lång sikt finns det stora brister som måste lösas innan det blir en lämplig teknik att använda. Eftersom det inte finns några vedertagna bättre lösningar för autenticering idag, rekommenderar trots allt vi att man bör använda digitala signaturer eftersom det trots allt ger bättre säkerhet än ingenting alls. Man bör också påbörja utvecklingsarbete av nya tekniker för autenticering så fort som möjligt. Detta för att möjliggöra en hållbar lösning för framtiden.

De problem som existerar idag är följande:

- Kort livslängd – digitala signaturer har en begränsad livslängd för att de algoritmer som byggt upp signaturen kan knäckas och förfalskas. Även korta nyckellängder spelar in här.
- Formatbyten – på grund av att digitala handlingar måste byta format blir den digitala signaturen ogiltig eftersom den beräknas på originaltexten.
- Certifikatshantering – en väl utbyggd hantering för certifiering av krypteringsnycklar måste finnas tillgänglig för att man ska kunna lita på att den digitala signaturen tillhör rätt person. Idag finns det oberoende organisationer som sköter certifikatshandlingen. Idag finns ingen garanti på att dessa organisationer finns kvar i framtiden.

Det finns olika förslag för att lösa dessa problem. När vi talar om livslängd på de digitala signaturerna finns det förslag att signera om de digitala handlingarna med nya signaturer, vilka över tiden även kan bli svårare att knäcka. Detta bör göras av arkiven med jämna mellanrum. Vi anser att detta förslag är väldigt realistiskt eftersom omsignering kan ske per automatik, vilket gör att arkiven själva inte behöver hantera den stora informationsmängden. Däremot anser vi att det är en temporär lösning. På detta sätt skjuter man bara problemet framåt i tiden och skapar mer administrativt arbete i framtiden.

För att lösa problemen med formatbyten finns det förslag om att spara information om hur handlingen har förändrats över tiden. Det är ett bra förslag enligt oss. Trots att det skapar mer arbete hjälper det till att upprätthålla autenticiteten i digitala handlingar. Vi ser däremot att det finns andra stora problem vid formatbyten. Vid varje formatbyte blir den digitala signaturen ogiltig och därför måste man omsignera handlingen. Innan denna omsignering görs måste den digitala handlingen granskas för att kunna avgöra om den

har förändrats vid formatbytet och på vilket sätt. Detta ger arkiven mycket merarbete vilket är ohållbart i längden.

Slutligen vad gäller certifikatshandlingen bör det finnas betrodda aktörer på marknaden som kan gå i god för att en krypteringsnyckel tillhör en viss person eller organisation. Idag fungerar detta utmärkt, men vi ser uppenbara problem med detta på lång sikt. Eftersom det är väldigt viktigt att dessa betrodda aktörer finns kvar i framtiden bör det finnas något centralt organ som har hand om certifieringen, till exempel en myndighet.

6.1.2 Realistiskt möjligt att implementera?

Den slutsats vi har kommit fram till i vår studie är att det är realistiskt möjligt att införa ett system för hantering av digitala signaturer i en arkivverksamhet. Eftersom att det är enkelt att införa, det oftast är kostnadseffektivt jämfört med tidigare rutiner samt att det är enkelt att använda blir det givetvis en realistisk möjlighet att implementera i verksamheten.

Det finns många faktorer att ta hänsyn till vid införande av ett system som ska verka på lång sikt, vilket oftast gör införandet väldigt komplext. Vi ser att det finns många faktorer ett arkiv måste ta hänsyn till innan själva införandet där de faktorer vi har påvisat i vår studie visar på att det faktiskt är realistiskt möjligt att införa ett system i arkivsammanhang.

Allt handlar dock inte om hur enkelt det är att införa utan man måste även ta hänsyn till kostnadsfrågor. Det är väldigt viktigt att kunna visa för ledningen på de vinster man kan göra i arkiven med hjälp av de nya systemen. Frågor som ”hur mycket kostar detta?” och ”vad tjänar vi på detta?” bör besvaras för att ledningen ska få en uppfattning om systemet. Ett alternativt sätt att angripa problemet är att dra paralleller till vad motsvarigheten, det vill säga vad lagring av pappershandlingar, kostar att administrera. Vid större volymer av handlingar bör således digitala system vara mer kostnadseffektiva än traditionella arkiv, eftersom de innehåller mindre manuella moment.

Användbarheten, alltså hur enkelt det är att använda systemet är också en viktig faktor. Vi anser att dessa system är stabila och lättanvända. Oftast märker inte den som använder systemet av den underliggande tekniken.

6.1.3 Trusted Archival Services – ett bra koncept?

Den slutsats vi har kommit fram till är att TAS är ett väldigt bra koncept för att upprätthålla autenticiteten för de digitala handlingar som arkiven har hand om. TAS har däremot vissa delar, exempelvis nyckelhantering vid formatbyten, som bör tänkas över av arkiven innan införande av konceptet. Vi anser att ett TAS löser problemen med autentisering av digitala handlingar på lång sikt.

Eftersom TAS förespråkar att arkiven bör omsignera sina handlingar med jämna mellanrum elimineras problemet med både formatbyte och kort livslängd hos den digitala signaturen. Däremot skapas det i fallet med formatbyte mycket extra arbete, men i dagsläget kan inte vi se någon bättre lösning för arkiven. Den korta livslängden hos digitala signaturer beror på att algoritmer kan knäckas, vilket i fallet med omsignering försvinner eftersom en ny signatur appliceras. Om arkivet ser att en krypteringsalgoritm

har knäckts kan de vidta åtgärder och signera om alla deras handlingar med en ny algoritm.

6.1.4 Diskussion om slutsatser

Att frågan om digitala signaturer är ett lämpligt sätt att lösa problematiken med autenticitet av digitala handlingar på lång sikt är viktig finns det ingen tvekan om. Enligt oss samverkar flera faktorer för att digitala signaturer överhuvudtaget ska vara ett alternativ. Som visats tidigare är det realistiskt möjligt att införa digitala signaturer i en organisation rent tekniskt, men det är även andra faktorer som spelar in. Att organisationer traditionellt sett är motståndare till förändringar tror vi kan påverka införandet. Om man för ledningen kan visa att införandet av ett system för hantering av digitala signaturer är enkelt att genomföra, att vinsterna blir högre med det nya systemet samt att det är väldigt enkelt att använda för personalen bör det bli lättare att driva genom ett införande. Det finns givetvis andra faktorer att ta hänsyn till också. Att digitala signaturer inte är ett lämpligt alternativ leder till att frågan om implementation blir mer komplicerad. Frågan blir ju isåfall om det är lämpligt att implementera något som inte är en hållbar lösning i längden.

Som visats har digitala signaturer flera problem som gör att det inte är en lämplig teknik för autentisering. Det handlar inte bara om tekniska aspekter, utan berör även andra aspekter. Säker hantering av digitala handlingar och dess signaturer är en aspekt, där arkiven kan använda sammanhangskontroll för att upprätthålla en säker hantering. En annan aspekt är den fysiska säkerheten som bör vara hög för att minska risken att någon obehörig kommer åt arkiven.

Vi tror att TAS är ett utmärkt sätt för arkiven att kunna upprätthålla autenticiteten i sina arkiv. Med hjälp av de krav som TAS ställer på ett arkiv elimineras också de flesta problem som digitala signaturer har. För att ett arkiv ska kunna tillämpa TAS krävs det att de tillhandahåller olika tjänster för användarna, men vi ser inte att detta är ett problem. Vi tror nämligen att arkiven är villiga att ta ansvar för autenticiteten hos deras handlingar. Vi kan också se att detta är en naturlig fortsättning på arkivens verksamhet, helt enkelt att ta ansvar för digitala handlingar på lång sikt. Att arkiven blir en betrodd certifierad tredjeparts aktör gör att autenticiteten upprätthålls ännu bättre. Vi ser att detta är väldigt viktigt för framtiden, då upphovsmannen till en digital handling kanske inte längre finns tillgänglig. Att då veta att arkivet är betrott ger en extra säkerhet för slutanvändaren.

Som vi ser det är inte digitala signaturer en lämplig teknik för autentisering av digitala handlingar på lång sikt. Detta eftersom det har flera problem. Om ett arkiv däremot tillämpar TAS elimineras dessa problem. Därför drar vi slutsatsen att digitala signaturer blir det lämpligaste alternativet att använda idag om det används i kombination med TAS. Dessutom förlänger TAS hållbarheten i arkiven. Detta leder till att chansen för att nya tekniker hinner utvecklas innan informationsmängden blir ohanterlig ökar, vilket också leder till att det blir mer lämpligt att implementera. Att system för digitala signaturer i sig dessutom är väldigt enkla att införa leder till att det inte bör vara några problem för arkiven att implementera i sin organisation.

6.2 Fortsatt forskning

I vår studie har vi sett att det finns behov av djupare studier inom detta område. Det skulle vara intressant att se vad det kostar i slutändan att implementera ett system för digitala signaturer om man betänker den långa tidsaspekten. I vår studie har vi undersökt om det är kostnadseffektivt på kort sikt, vi har inte tänkt på de faktorer som spelar in på lång sikt. En sådan faktor kan till exempel vara att systemen måste bytas ut över tiden eftersom digitala signaturer inte är en lämplig teknik i längden.

En annan intressant fråga är att praktiskt införa och testa ett TAS i ett arkiv. Eftersom det inte har utförts några praktiska studier på TAS skulle det vara intressant att se utfallet av en sådan studie.

6.3 Metoddiskussion

Här kommer vi att diskutera på vilket sätt allt arbete med vår studie har fallit ut. Vi kommer att titta dels på vilken litteratur vi har använt, men även på vilka respondenter vi har valt ut och vilka frågor vi ställde till dessa respondenter. Slutligen redogör vi för vår syn på de slutsatser vi har dragit.

6.3.1 Teori

Eftersom det ämnesområde vi har valt att inrikta oss på är tunt har det varit vissa svårigheter med att hitta relevant material. Efter att ha försökt hitta information i skrivna böcker har vi fått söka oss ut på Internet för att söka i artikeldatabaser. I dessa databaser har vi hittat ganska mycket relevant litteratur som har kulminerat i den teoretiska referensram vi har med i vår studie. Trots den begränsade tillgången av litteratur i bokform är vi ändå nöjda med materialet till vår studie. Att använda sig av artikeldatabaser för forskning istället för äldre skrivna böcker anser vi ger denna studie mer trovärdighet och tyngd till våra argument.

6.3.2 Undersökningsobjekt

I vår rapport har vi gjort en del val som vi inte är riktigt nöjda med. Vi valde ut några lämpliga respondenter enligt vårt tycke, där några tyvärr inte ville eller hade möjlighet att vara med. På grund av detta fick vi fråga de respondenter som vi fick tag på efter nya namn att intervjuas. Detta behöver inte vara ett sämre alternativ, men vi är väl medvetna om att detta kan ha påverkat resultatet eftersom några av respondenterna arbetar på samma ställe. Däremot vet vi inte om detta har påverkat resultatet positivt eller negativt. Om studien ska göras om i framtiden bör ett större urval definitivt väljas ut. Framförallt ger det mer tyngd åt det empiriska materialet, men det är även bra ur en praktisk synvinkel med fler respondenter utifall någon eller några inte kan ställa upp. Trots de stora problem vi har haft med våra initiala respondenter tycker vi att det empiriska material vi har samlat in har tyngd. Alla våra respondenter är väl insatta i begreppet långsiktigt digitalt bevarande och de har arbetat inom detta område i flera år.

6.3.3 Intervjufrågor

En sak som fungerade bra är intervjuerna. Det hjälpte oerhört mycket att använda sig av en intervjuguide för att genomföra intervjuerna. Frågorna i intervjuguiden kom vi fram

till genom att knyta problemdiskussionen mot teorin och därifrån dra slutsatser om vilka frågor som behövde ställas. För att säkerställa kvaliteten på intervjuguiden testade vi den på en forskare inom området vilken höll med om att vi ställde relevanta frågor. Hade vi fått göra om denna studie hade vi använt oss av fler pilotfall då några av frågorna fick strykas vid senare tillfälle då vi kände att de inte var riktigt relevanta för våra forskningsfrågor.

6.3.4 Slutsatser

De slutsatser vi har kunnat dra i denna studie anser vi vara giltiga. Vi har använt oss av personer med mycket kunskap på området och vedertagen teori som stöd för att kunna dra våra slutsatser. För att kunna dra generella giltiga slutsatser anser vi dock att vår studie borde ha haft ett större antal respondenter för det empiriska materialet. Vi tror ändå att våra slutsatser bör kunna ge en fingervisning om hur relevant digitala signaturer är för långsiktigt digitalt bevarande.

7. Referenslista

7.1 Bokreferenser

- Andersson, S. (1979) *Positivism kontra Hermeneutik*. Korpen: Göteborg.
- Artsberg, K. (2003) *Redovisningsteori – policy och praxis*. Liber ekonomi: Berlings skogs: Trelleborg.
- Bryman, A. (2002) *Samhällsvetenskapliga metoder*. Liber ekonomi. Berlings skogs: Trelleborg.
- Friedman, A., Cornford, D. (1989) *Computer Systems Development - History, Organisation and Implementation*. Wiley: Chichester.
- Jacobsen, D-I. (2002) *Var, hur och varför?* Studentlitteratur: Lund.
- Jensen, K. (1995) *Kvalitativa metoder för samhälls- och beteendevetare*. Studentlitteratur: Lund.
- Moriso, M., Seaman, C.B., Basili, V.R., Parra, A.T., Kraft, S.E., Condon, S.E. (2002) *COTS-based software development: Processes and open issues*. Journal of Systems and Software Vol. 61 Issue 3: pp. 189-199.
- Nielsen, J. (2001) *Användbar Webbdesign*. Liber: Stockholm.
- Patel, R., Tebelius, U. (1987) *Grundbok i forskningsmetodik*. Studentlitteratur: Lund.
- Patel, R., Davidsson, B. (1994) *Forskningsmetodikens grunder*. Studentlitteratur: Lund.
- Regeringskansliet. (1998) *Digitala signaturer – en teknisk och juridisk översikt*. Regeringskansliets offsetcentral: Stockholm.
- Werr, A., Stjernberg, T., Docherty, P. (1995) *Att förändra strukturer – en översikt och jämförelse*. I Löwstedt. *Människan och strukturerna*. Nerenius & Santérus: Stockholm.

7.2 Internetreferenser

- Arkivutredningen. (2000) *Arkiv för alla*. Tillgänglig på Internet:
http://ldb.project.ltu.se/main.php/Arkivutredning%202002_78.pdf?fileitem=6045827.
Hämtad [2006.10.27]
- Dobratz, S., Schoger, A. (2005) *Digital Repository Certification: A Report from Germany*. Tillgänglig på Internet:
<http://edoc.hu-berlin.de/oa/articles/reh7CbxRopdUA/PDF/23yn183UoMBU.pdf>.
Hämtad [2006.11.04]

Dumortier, J., Van den Eynde, S. (2005) *Electronic Signatures and Trusted Archival Services*. Tillgänglig på Internet: <http://www.law.kuleuven.ac.be/icri/publications/172DLM2002.pdf?where=&temp=22a32cc7af0c91bc1df5ca4417ec4985>. Hämtad [2006.11.05]

Dumortier, J., Libon, O., Mitrakas, A., Schreiber, A., Van Eecke, P., Van den Eynde, S. (2000) *Trusted Archival Services*. Tillgänglig på Internet: <http://www.law.kuleuven.ac.be/icri/publications/91TAS-Report.pdf>. Hämtad [2006.11.06]

Heslop, H., David, S., Wilson, A. (2002) *An Approach to the Preservation of Digital Records*. Tillgänglig på Internet: http://www.naa.gov.au/recordkeeping/er/digital_preservation/Green_Paper.pdf. Hämtad [2006.11.10]

Hofman, H. (2003) *Can Bits and Bytes be Authentic? Preserving the Authenticity of Digital Objects*. Tillgänglig på Internet: http://eprints.erpanet.org/39/01/hofman_glasgow02.pdf. Hämtad [2006.11.04]

Lekkas, D., Gritzalis, D. (2004) *Cumulative Notarization for Long-term Preservation of Digital Signatures*. Tillgänglig på Internet: <http://www.syros.aegean.gr/users/lekkas/pubs/j/2004COMPSEC.pdf>. Hämtad [2006.10.27]

Linder, J. (2003) *Förslag på tillämpning av Försvarsmaktens IS/IT-livscykelmodell – Med hänsyn tagen till Försvarsmaktens krav på informationssäkerhet*. Tillgänglig på Internet: <http://www.dsv.su.se/research/seclab/pages/pdf-files/04-23.pdf>. Hämtad [2006.11.05]

Lynch, C. (1999) *Canonicalization: A Fundamental Tool to Facilitate Preservation and Management of Digital Information*. Tillgänglig på Internet: <http://www.dlib.org/dlib/september99/09lynch.html>. Hämtad [2006.11.05]

Rivest, R-L., Shamir, A., Adleman, L. (1978) *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Tillgänglig på Internet: <http://delivery.acm.org/10.1145/360000/359342/p120rvest.pdf?key1=359342&key2=5100693611&coll=GUIDE&dl=GUIDE&CFID=6540216&CFTOKEN=58842441>. Hämtad [2006.11.20]

RLG-OCLC. (2002) *Trusted Digital Repositories: Attributes and Responsibilities*. Tillgänglig på Internet: <http://www.rlg.org/legacy/longterm/repositories.pdf>. Hämtad [2006.11.15]

Rothenberg, J. (2000) *Authenticity in a Digital Environment*. Tillgänglig på Internet: <http://www.clir.org/pubs/reports/pub92/pub92.pdf>. Hämtad [2006.11.05]

Runardotter, M., Quisbert, H., Nilsson, J., Hägerfors, A., Mirijamdotter, A. (2005) *The Information Life Cycle – Issues in Long-term Digital Preservation*. Tillgänglig på Internet: <http://www.hia.no/iris28/Docs/IRIS2028-1044.pdf>. Hämtad [2006.12.01]

Runardotter, M. (2007) *Information Technology, Archives and Archivists – An Interacting Trinity for Long-term Digital Preservation* Tillgänglig på Internet: <http://epubl.ltu.se/1402-1757/2007/08/LTU-LIC-0708-SE.pdf> Hämtad [2007.03.23]

Sundgren, D. (2003) *Offentlig upphandling av komplexa IT-system i elbranchen – Skapar lagen affärsmässiga upphandlingar?* Tillgänglig på Internet: http://www.diva-portal.org/diva/getDocument=urn_nbn_se_kth_diva-1678-2_fulltext.pdf Hämtad [2007.03.23]

Wickström, F. (2004) *Digital vattenmärkning*. Tillgänglig på Internet: http://www.nada.kth.se/utbildning/grukth/exjobb/rapportlistor/2004/rapporter04/wickstrom_fredrik_04079.pdf. Hämtad [2006.11.01]

8. Bilagor

8.1 Intervjuguide

Långsiktigt Digitalt Bevarande

- Vilka problem ser du med autentisering av digitala handlingar i framtiden med tanke på teknikens utveckling?
 - Hur skulle du vilja göra för att höja autenticiteten för digitala handlingar?

Digitala Signaturer

- Tycker du att digitala signaturer är en lämplig teknik för autentisering?
 - Stödjer digitala signaturer en handlingens identitet?
 - Stödjer digitala signaturer en handlingens integritet?
 - Är digitala signaturer ett kostnadseffektivt sätt att hantera dessa frågor?
 - Är det enkelt att införa och använda i arkiv?
- Vilka problem ser du med digitala signaturer i samband med långsiktigt digitalt bevarande?
 - Finns det några andra problem (ex säkerhet, livslängd)
- Vattenmärkning, Vad anser du om detta alternativ?
 - Ser du några problem med denna typ av digital signatur?
 - Skulle det vara ett bra alternativ om man bortser från att handlingen förändras? (inte är legal)
 - Är det dåligt att handlingen förändras?
- Assymetrisk kryptering och hash-summor, vad anser du om dessa två alternativ?
 - Ser du några problem med dessa typer av digitala signaturer?

TAS

- Har du hört talas om TAS?
- Vad anser du allmänt om TAS?
- Tror du att TAS löser dagens befintliga problem med digitala signaturer?
- Vad anser du om kraven som ställs på ett TAS?
 - Handlingens format
 - Teknologisk interoperabilitet
 - Bakåtkompatibilitet
 - Kryptografisk uppföljning
- Kommer de arkiv som används idag vara villiga att ta ansvar för att digitala signaturer och handlingar är valida och säkra?
- Finns det något i TAS som inte är realistiskt?
 - Vad skulle du ändra på i TAS om du hade möjlighet?
 - Kan det göras på något annat sätt?

- Vilken av TAS två modeller anser du är bäst för bevarande av digitala handlingar? (centraliserad / distribuerad)

Allmänt

- Har du några allmänna synpunkter på detta område?