GÖTEBORGS UNIVERSITET

Distribution av känslig data

En fallstudie i distribution av data mellan försvarsföretag och militära kunder

Distribution of sensitive data

A case study in data distributions among defense companies and military customers

SIMON EINBEIGI
JOHAN PETERSÉN

Rapport nr: 2013:059
ISSN: 1651-4769

Kandidatuppsats i Informatik V13

Göteborgs universitet
Institutionen för tillämpad informationsteknologi
Göteborg, Sverige, Maj 2013

Abstract

Informationsteknologi (IT) gör det möjligt att elektroniskt distribuera data mellan aktörer som befinner sig i geografiskt skilda områden. Nuförtiden skickas information allt mer sällan via traditionella brevförsändelser till förmån av snabbare elektroniska motsvarigheter via internet.

Trots effektiv IT - miljö och säkra krypteringstekniker väljer vissa aktörer att skicka information genom fysisk överlämning. Detta fenomen förekommer hos aktörer som arbetar med sekretessbelagd information eftersom den ska hanteras efter ett antal regler och säkerhetsskrifter.

Utifrån en uppsättning regler och krav har vi sett över möjligheten att skicka känslig information elektroniskt över internet. Syftet var att finna generella riktlinjer för hur företag och organisationer bör hantera och skicka känslig information över osäkra nätverk. Detta ledde oss till vår forskningsfråga; Hur kan information som utbyts mellan aktörer i geografiskt skilda områden kategoriseras och krypteras så att den kan transporteras över internet utan säkerhet eller integritetsbrister?

För att besvara frågeställningen genomfördes en fallstudie på ett försvarsföretag. Utifrån de förutsättningar och krav har generella riktlinjer tagits fram med hjälp existerande tekniker och teorier informationssäkerhet.

Av fallstudien kom vi fram till att om aktörer har en förståelse för informations värde är det lättare att sätta ta fram riktlinjer för hur den bör hanteras av olika personer och system. I nuläget är informationsteknologi ett såpass utvecklat område så att den inte anses som ett hinder för att möjliggöra säker lagring, distribution eller bearbetning av känslig data. Det största utmaningen är istället de administrativa åtgärder som krävs för att få en förståelse för hur information ska hanteras innan- och utanför organisationen. Genom att förstå värdet på informationen är det lättare att föreslå vilka tekniska alternativ som kan användas för att uppnå önskat resultat.

Nyckelord; *Distribution av data, informationssäkerhet, kryptering, filöverföringsprotokoll, sekretessbelagd information.*

Abstract

Information Technology (IT) makes it possible to electronically distribute data between actors who are in geographically diverse areas. Nowadays, information is sent less frequently through traditional correspondence in favor of faster electronic equivalents via the internet.
Despite effective IT - environment and secure encryption techniques choose some actors to send information through physical delivery. This phenomenon occurs in those working with confidential information as it is handled by a number of rules and safety regulations.

Based on a set of rules and requirements, we have looked over the possibility of sending sensitive information electronically over the internet. The aim was to find general guidelines for how companies and organizations should manage and send sensitive information over insecure networks. This led us to our research question: How can information be exchanged between actors in geographically diverse areas be categorized and encrypted so that it can be transported over the internet without security or integrity deficiencies?

To answer the question, there was a case study at a defense company. Based on the assumptions and requirements have general guidelines been developed using existing technologies and theories of informationsecurity.

Based on the case study, we concluded that if actors have an understanding of information value, it is easier to set up general guidelines for how it should be handled by different people and systems.
At present, information technology a whim developed area so that it is not considered as an obstacle to enable secure storage, distribution and processing of sensitive data. The biggest challenge is instead the administrative steps required to get an understanding of how information should be handled before and outside of the organization. By understanding the value of the information is easier to propose the technical options that can be used to achieve the desired results.

Keywords: *Distribution of data, information security, encryption, file transfer protocol, classified information.*

Tack till

Vi vill tacka Henrik Fagrell på Diadrom Systems AB för intiativ till detta arbete och för hjälpen med att hitta lämpliga kontaktpersoner. Dessa personer vill vi också tacka för att ni gav oss input till uppsatsens resultat. Slutligen vill vi tacka vår handledare Urban Nuldén för ovärderlig feedback under studiens arbetsgång.

Innehållsförteckning

1 Inledning

Informationsteknologi(IT) gör det möjligt att elektroniskt distribuera data mellan aktörer som befinner sig i geografiskt skilda områden. Nuförtiden skickas information allt mer sällan via brevförsändelser till förmån av snabbare elektroniska motsvarigheter via internet. Eftersom det vid elektronisk överföring finns möjlighet att avlyssna och ta del av innehållet är det nödvändigt att göra meddelandet obegripligt för en obehörig. Ett vanligt sätt att göra data obegriplig är genom att överföra det till hemlig kod med hjälp av kryptering (Frank, 2011).

Trots effektiv IT - miljö och säkra krypteringstekniker väljer vissa aktörer att skicka information genom fysisk överlämning (Broman & Lindgren, 2004). Detta fenomen framträder tydligt hos aktörer som arbetar med sekretessbelagd information eftersom den ska hanteras efter ett antal regler och säkerhetsskrifter (Hallén & Larsson, 2010; Försvarshögskolan, 2013-04-20). Krav på informationssäkerhet varierar hos olika företag och organisationer. Försvarsindustrin är ett område där man ställer höga krav på säkerhet eftersom säkerhetsbrister kan leda till ekonomiska konsekvenser och minskad trovärdighet. I särskilda fall kan dataförluster även påverka nationers trygghet.

Mot bakgrund av ovanstående vill vi se över möjligheten att på ett säkert sätt skicka känslig information mellan olika företag och organisationer över internet. En elektronisk lösning kan i de flesta fall ge företag högre tillgänglighet på information och kan därmed med högre precision föreslå åtgärder som krävs i sammanhanget.

För att ta reda på hur det kan gå till och för att få förankring till verkligheten har vi valt att utföra en fallstudie av ett företag som är verksam inom försvarsindustrin. Henrik Fagrell, VD på Diadrom har mångårig erfarenhet av att arbeta med försvarsföretaget och har god kännedom om deras nuvarande arbetssätt. Information som vi fått från Diadrom och Henrik Fagrell kommer att spela en central roll i vårt fortsatta arbete med att ta framlösningsförslag till försvarsföretaget. Av fallstudien hoppas vi på att kunna ta fram generella riktlinjer för hur företag och organisationer bör hantera och distribuera sekretessbelagd information över internet.

1.1 Problem

Aktörer som arbetar med sekretessbelagd information ansvarar själva för att utforma, dokumentera och införa riktlinjer för hur information ska hanteras (Hallén & Larsson, 2010). Trots att organisationer och företag numera hanterar stora mängder data med hjälp av IT, väljer vissa aktörer att skicka känslig information genom fysisk överlämning. En verksamhets framgång handlar ofta om att effektivt kunna leverera information till rätt ställe och vid rätt tidpunkt. Denna effektivitet nås lättast genom att reducera

de icke värdeskapande aktiviteterna, där bland annat distribution av data (Broman & Lindgren, 2004).

Antalet inbyggda system (engelskans embedded systems) ökar starkt och används i stor utsträckning av bland annat fordon- och flygindustrin. Inbyggda system avser datorer som ansvarar för en eller ett fåtal funktioner och är ofta en del av en maskin eller apparat. Datorerna kan till exempel ansvara för en bils diagnostik och meddela föraren vid mekaniska och elektroniska avvikelser (Seshadri, A et.al).

Ett företag som är verksam inom försvarsindustrin levererar vapensystem till flera nationer. Den senaste versionen av vapensystemet har många inbyggda datorer som kan logga driftparametrar. I nuvarande situation är processen för att erhålla driftinformation komplicerad och kostnadskrävande. Konstruktionen av systemet är avancerad och gör det nödvändigt för försvarsföretaget att utbilda militära kunder på plats i hur man kommer åt driftparametrar. Eftersom parametrarna innehåller känslig information ställs det höga krav på informationssäkerhet vid distributionsprocessen. I nuläget skickas information manuellt med hjälp av kurirer och diplomatpost, vilket är en kostsam och tidskrävande process.

En elektronisk lösning för distribution av data kan effektivisera utbytet av information mellan försvarsföretag och militära kunder. Genom att ge försvarsföretaget högre tillgänglighet på kunders vapensystem skulle dem kunna tillgodose reservdelar och underhållsåtgärder med högre precision.

1.3 Syfte och frågeställning

I undersökningen vill vi utifrån en uppsättning regler och krav se över möjligheten elektroniskt skicka känslig information över internet. Syftet är att finna generella riktlinjer för säker hantering och distribution av känslig data mellan aktörer i geografiskt skilda områden. Med lösningen vill vi få fler aktörer att använda digitala alternativ för överföringar av känslig data framför traditionella försändelser.

Frågeställningen lyder:
Hur kan information som utbyts mellan aktörer i geografiskt skilda områden kategoriseras och krypteras så att den kan transporteras över internet utan säkerhet- och integritetsbrister?

För att besvara ovanstående forskningsfråga har vi utfört en fallstudie av ett företag som är verksamma inom försvarsindustrin (se fallstudie kapitel 3.1). I fallstudien vill vi se över möjligheten att skicka driftinformation om vapensystem mellan militära kunder och försvarsindustrin över internet. En elektronisk lösning kan i fallet ge försvarsföretaget högre tillgänglighet på vapensystem och därmed balansera behovet av reservdelar och serviceåtgärder baserat på hur systemet används.

I dokumentet har försvarsföretagets identitet anonymiserats på grund av sekretess- och säkerhetsskäl. Anonymiseringen påverkar dock inte studiens resultat eftersom lösningen ska kunna generaliseras för att

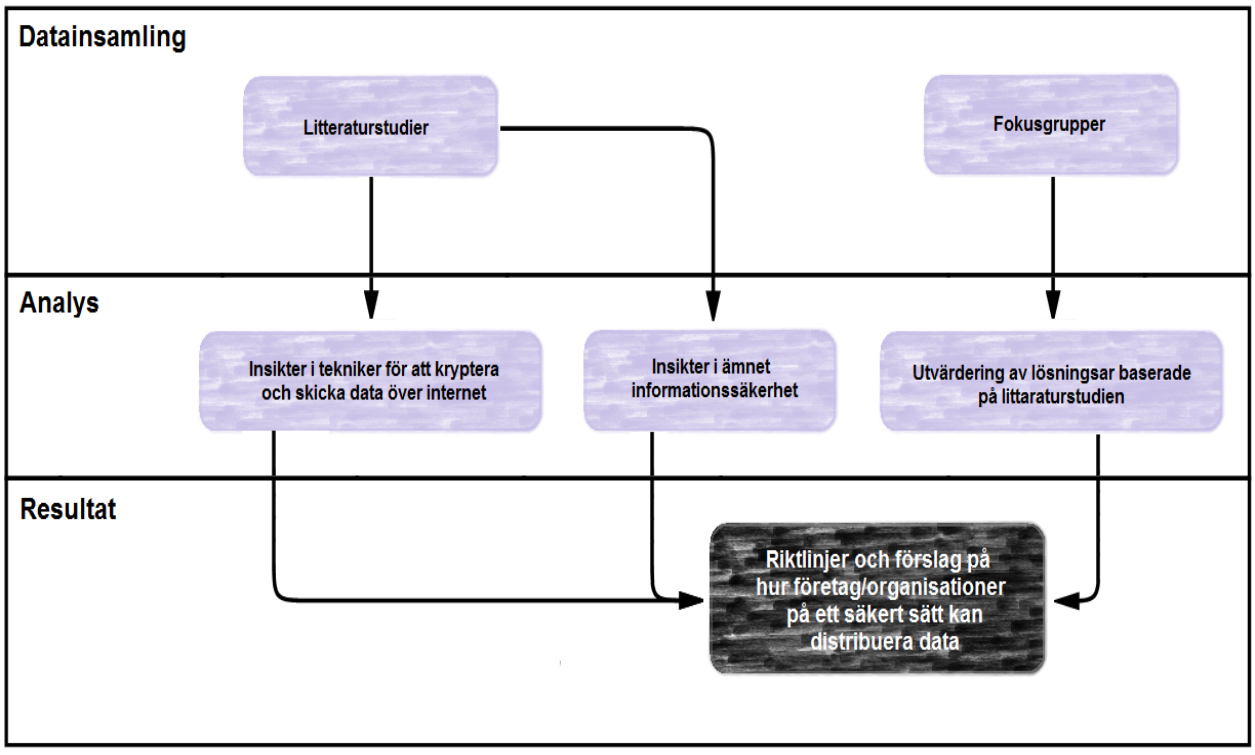
kunna appliceras på fall med liknande kontext. Däremot är det svårt för läsaren att kontrollera studiens referenser eftersom hänvisning till specifika personer inte publiceras.

1.4 Avgränsning

I denna uppsats har vi valt att avgränsa oss till kryptering och kategorisering av information samt hantering av nycklar för att säkerställa säker distribution av data. Vi kommer därför inte att resonera omkring diverse säkerhetslösningar som kan förhindra intrång i datalager. Vidare bortser vi att beakta organisationens interna riktlinjer för att skydda sig mot externa hot.

1.5 Undersökningens upplägg

Figur 1.1 ger en översikt om hur vi ser den här studiens upplägg. I kapitel 2 presenteras relaterat arbete och förväntas ge insikter i ämnet informationssäkerhet och tekniker som används för att kryptera och skicka data över internet. I kapitel 3 görs en presentation av vår fallstudie och metodvalen som vi har använt oss av för att samla in och bearbeta information. Med hjälp av dessa hoppas vi på att kunna utvärdera och samla information för att få en ökad förståelse för dem aspekter som är viktiga att ta hänsyn till när man handskas med känslig information. Därigenom väntar vi oss att kunna utforma generella riktlinjer för hur företag och organisationer på ett säkert sätt kan hantera och skicka data över internet. Resultatet av fallstudien presenteras i kapitel 4 som vi sedan håller ett analyserande resonemang om i kapitel 5. Slutligen redovisas källor i kapitel 6.



Figur 1.1 vy av studiens upplägg.

2 Relaterat arbete

I detta kapitel kommer vi att beskriva existerande alternativ för att möjliggöra säker distribution av information. Vi kommer att lyfta fram delar som omfattar hur organisationer skapar värde av, och bestämmer informationens känslighet. Vidare beskriver vi alternativ för hur känslig information kan krypteras och distribueras för att minska risken för att en obehörig kan förstå den.

2.1 Informationssäkerhet

Informationssäkerhet är ett brett ämnesområde med många infallsvinklar och omfattar bland annat åtgärder för att minska risken för hot mot informations sekretess, tillgänglighet, riktighet och spårbarhet (Hallén & Larsson, 2010). Det finns olika delar av skydd som organisationer och företag behöver se över. Generellt kategoriseras dessa under; förebyggande åtgärder som går ut på att förhindra att en händelse inträffar; begränsande åtgärder vilket innebär att organisationen minskar skadan vid ett eventuellt intrång; och rapporterande åtgärder som menas att organisationen märker av när ett intrång sker i deras egna system. Dessa delas i sin tur in under logiska- och administrativa åtgärder. Logiska åtgärder beskriver hur organisationen kan uppnå säker informationshantering med hjälp av implementering av tekniska säkerhetslösningar, exempelvis genom kryptering och autentiseringslösningar. Administrativa åtgärder innebär istället att organisationen fastställer regler, krav, riktlinjer samt instruktioner för hur information får hanteras. De administrativa åtgärderna omfattar inte sällan klassificering av information, vilket en viktig process eftersom det ligger till grund för arbetet med att ta fram regler om hur information ska handskas inom organisationen (Hallén & Larsson, 2010).

2.1.1 Klassificering av information

Organisationer distribuerar och hanterar idag stora mängder information med hjälp av informationsteknologi. IT-systemen används sällan till fullo och organisationerna är inte insatta i hur mycket information som dessa tillhandahåller. Till skillnad från fysiska produkter så är det svårt att sätta ett värde på informationen. Beroende på i vilket sammanhang som information används varierar dess värde. För att organisationer ska kunna skydda den information som anses värdefull behöver den klassificeras (Hallén & Larsson, 2010; Myndigheten för samhällsskydd och beredskap, 2013-05-14).

Vid genomförande av informationsklassificering ges ett värde till varje informationskategori beroende på känslighetsgrad. När klassificeringen av informationen är genomförd kan organisationen fastställa vilka säkerhetskrav som ska ställas på lagring, hantering och personer som ska ha åtkomst till den. Organisationer som arbetar med information som vid förluster kan anses som ett hot mot nationen eller personers integritet kan tvingas att följa vissa regelverk som är fastställda av myndigheter, eller ISO - standarder som innehåller rekommendationer om hur man kan uppnå säkerhet inom särskilda områden (Hallén & Larsson, 2010).

Figur 2.1 visar hur informationsklassificering ser ut inom vissa delar av det svenska försvaret (Försvarshögskolan, 2013-04-20).

"Generellt är klassificering av information viktig att kartlägga eftersom det styr hur information ska hanteras och vilka krav som ställs på personal som hanterar den" (Försvarsföretaget).

Informationssäkerhetsklass	Förkortas	Motsvarar tidigare	Vid informationsförlust
HEMLIG/TOP SECRET	H/TS	Kvalificerat hemlig	synnerligt men
HEMLIG/SECRET	H/S	Hemlig	betydande men
HEMLIG/CONFIDENTIAL	H/C	Saknas	icke obetydligt men
HEMLIG/RESTRICTED	H/R	Saknas	ringa men

Figur 2.1 exempel av informationsklassificering.

2.2 Kryptering av information

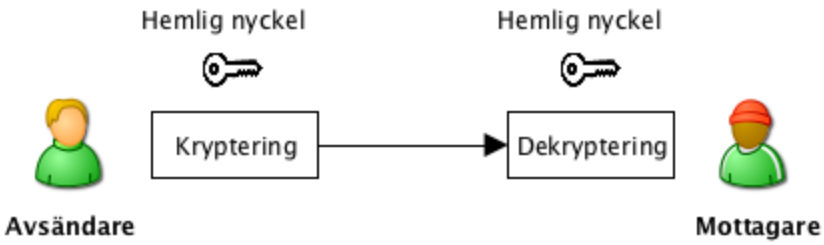
Kryptering är en samling tekniker för att manipulera information. Vid kryptering innebär det att man gör ett meddelande obegripligt genom att överföra det till hemlig kod. Dekryptering gör motsatsen och återställer ett krypterat meddelande till begriplig information. För att kryptera och dekryptera ett meddelande krävs en nyckel samt en krypteringsalgoritm (kallas även för chiffer). Genom att applicera algoritmen på ett meddelande skapas krypterad information. För att återställa ett manipulerat meddelande till sitt ursprung behöver mottagaren använda sig av en dekrypteringsnyckel. Kryptering av känslig information är viktigt när den skickas över internet eftersom det finns en risk att en obehörig kan komma åt den (Frank, 2011).

Vid kryptering och dekryptering används nycklar som består av en uppsättning tecken. Dessa tecken är speciella för varje enskild avsändare och mottagare. I vissa fall är nyckeln samma för både sändare och mottagare, en så kallad hemlig nyckel. Det är viktigt att hålla dekrypteringsnyckeln gömd för obehöriga då den används för att omvandla krypterade meddelanden till klartext. När man använder hemliga

nycklar är det extra viktigt då man kan bestämma nycklarna ur varandra (Frank, 2011).

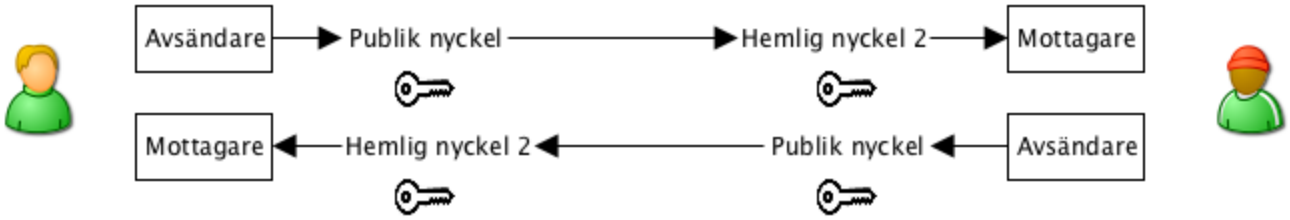
2.2.1 Symmetrisk och asymmetrisk kryptering

Man skiljer på symmetrisk och asymmetrisk kryptering. Vid symmetrisk kryptering så använder avsändare och mottagare hemliga nycklar både vid kryptering och dekryptering av ett meddelande. Genom att kryptera känslig information symmetriskt ställs det höga krav på att nycklarna förvaras på ett säkert sätt. Då flera personer använder sig av samma nyckel ökar risken för att obehöriga kommer åt dem. Obehöriga aktörer som kommer över en hemlig krypteringsnyckel kan även dekryptera meddelandet (Frank, 2011).



Figur 2.1.1 översikt av symmetrisk kryptering. Avsändaren krypterar meddelandet med sin hemliga nyckel och mottagaren dekrypterar med sin identiska nyckel.

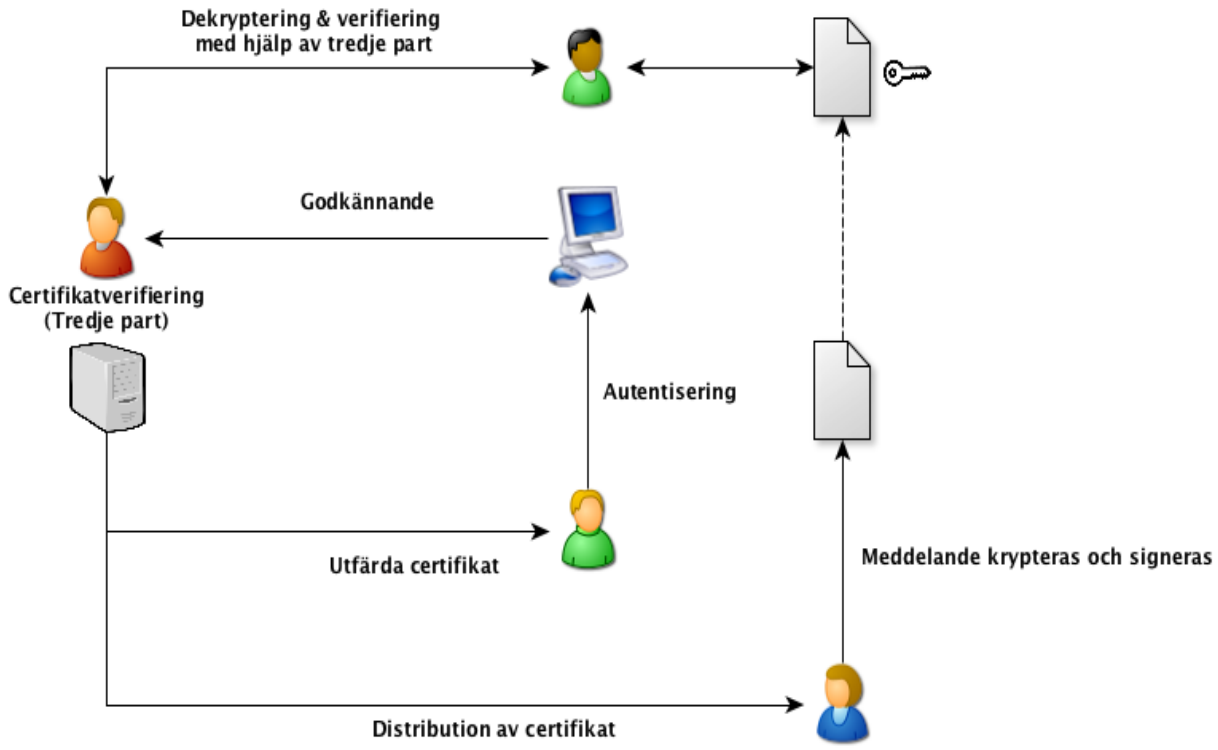
Vid asymmetrisk kryptering så använder sig avsändare och mottagare av både publika och hemliga nycklar. Den publika nyckeln i asymmetrisk kryptering behöver inte hållas gömd då den skiljer sig från den hemliga nyckel som behövs för att dekryptera meddelandet. Asymmetriska krypteringsnycklar är utformade parvis där man med hjälp av den publika nyckeln kan kryptera information och mottagaren kan dekryptera informationen med den hemliga nyckeln i paret (Frank, 2011).



Figur 2.1.2 översikt av asymmetrisk kryptering. Avsändaren krypterar meddelandet med en publik nyckel och mottagaren dekryptera med sin hemliga nyckel. En uppsättning nycklar för att skicka och en annan för att ta emot.

2.2.1.1 Certifiering av nycklar med PKI (Public Key Infrastructure)

PKI, Public Key Infrastructure är ett alternativ för att hantera publika krypteringsnycklar. Lösningen ger användaren möjlighet att distribuera asymmetrisk krypterad (se asymmetrisk kryptering kapitel 2.2.1) information över osäkra nätverk, till exempel internet. Användarens publika nyckel binds ihop med dess användaruppgifter, detta bildar ett digitalt certifikat. Certifikaten blir verifierade av en tredje part som användarna anser är tillförlitlig, även den här personen har uppgifter kopplade till en publik nyckel. Detta leder till att andra användare kan lita på signaturer som görs med den privata nyckeln som tillhör den publika nyckeln som certifikatet har verifierat. Avsändare som innehar ett certifikat kan identifiera sig mot servrar (se FTPS kapitel 2.3), med hjälp av signering med sin privata nyckel. Med detta kan användare åstadkomma en säker plats att dela information. PKI tillåter åtkomst till stationära system vid användning av smart card (se smart card kapitel 2.2) med hjälp av detta kan man vara säker på att rätt person använder systemet (Andersson, 2002).



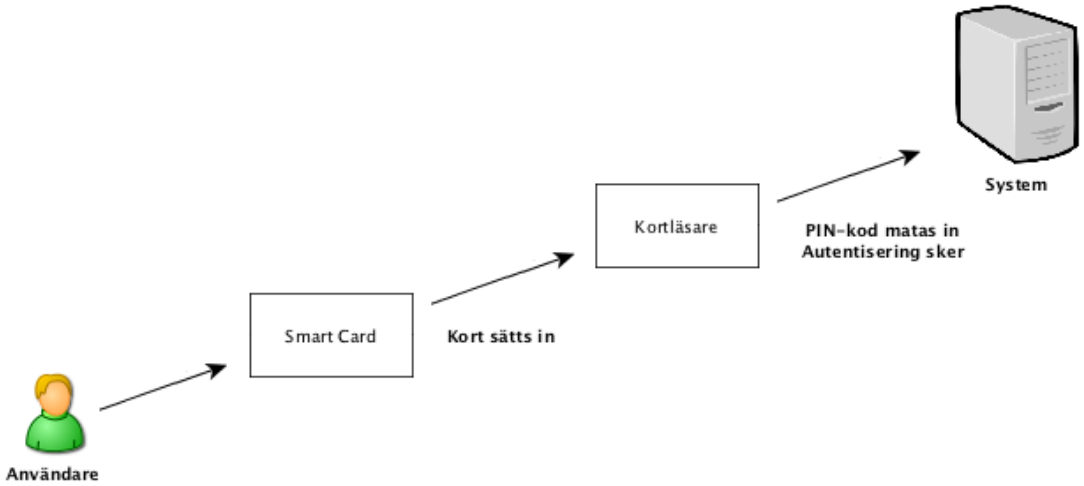
Figur 2.2.1.1 Beskriver verifiering av certifikat

2.2.1.2 Signering med krypteringsalgortimen RSA

RSA - kryptering är en av de krypteringsalgoritmer som används frekvent. Fördelen med att använda en asymmetrisk algoritm som RSA är att avsändaren kan signera meddelandet. Avsändaren använder sin hemliga nyckel tillsammans med den fastställda algoritmen för skapa ett hashvärde. Ett hasvärde tas fram med en algoritm som omvandlar information till ett heltal. Meddelandet och hashvärdet skickas sedan till mottagaren som med hjälp av avsändarens publika nyckel kan dekryptera hashvärdet. Mottagaren genomför själv en beräkning av hashvärdet och ställer det mot avsändarens och stämmer de överens så kan mottagaren säkerställa att meddelandet kom från rätt person. Nackdelen med RSA är att krypteringsalgoritmen är långsam (Ehsas, 2011).

2.2 Autentisering med smart card

Smart card är en säkerhetslösning som möjliggör autentisering via ett aktivt kort. Lösningen kan liknas vid ett kreditkort då varje kort är unikt och erfordrar PIN-kod. I kortets minne återfinns ytterligare en säkerhetsåtgärd i form av en hemlig krypteringsnyckel som vid användning autentiserar att användaren är behörig. Den här lösningen används tillsammans med en kortläsare kopplad till systemet där användaren sätter i kortet och uppger PIN-kod. Stämmer koden och den hemliga nyckeln få användaren tillgång till systemet. Smart card använder sig av asymmetrisk kryptering där kortet har en hemlig nyckel och en systemet användaren integrerar med har en publik nyckel. Man kan säga att smart card innehåller flera olika säkerhetslösningar eftersom kortet med tillhörande PIN-kod är unikt för varje användare och autentiseras då krypteringsnycklarna stämmer överens. Fördelen med att använda smart card är att man med säkerhet kan avgöra att det är en behörig användare som får åtkomst till systemet med hjälp av ovanstående aspekter. Däremot är lösningen i behov av ytterligare hårdvara i form av kortläsaren för att lösningen ska kunna fungera, vilket kan anses vara en nackdel (Hansson, 2009; Frank, 2011).



Figur 2.2 beskriver autentisering med smartcard. Användaren sätter in sitt smart card i kortläsaren och matar in PIN-kod, autentisering sker med hjälp av kod och krypteringsnyckel.

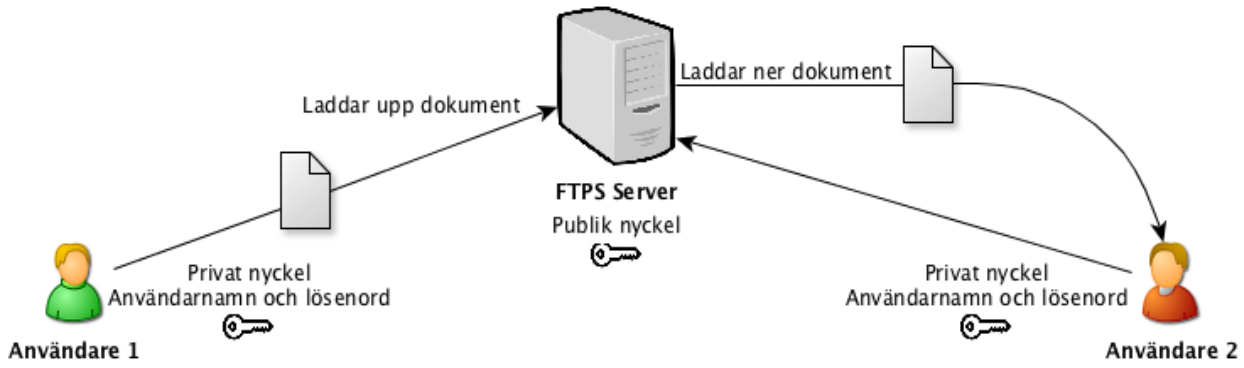
2.3 FTP (File Transfer Protocol)

FTP, File Transfer Protocol är en applikation som används för att transportera filer mellan användare och system, via lokala nätverk eller över internet. FTP är plattformsoberoende vilket gör det möjligt att flytta information mellan olika system. De enklare typerna av FTP har inga säkerhetslösningar och innehåller ingen form av kryptering vilket medför att information skickas i klartext och gör det lätt för en obehörig att komma åt den (Pettersson, 2008).

FTPS, SSL File Transfer Protocol är ett säkrare alternativ av de tidiga FTP applikationerna.

Den användare som vill göra en fil tillgänglig för andra användare kan med hjälp av sin privata krypteringsnyckel, samt ett användarnamn och lösenord få tillgång till FTP-servern. När filen ligger på servern kan övriga som har tillgång till servern gå in med sina privata nycklar, användarnamn och lösenord koppla upp sig mot servern för att ladda ner filen (Botrakoff, 2009).

Det är vanligt förekommande att organisationer använder sig av detta för sprida relevant information till anställda och kunder (Westin, 2011).



Figur 2.3 Beskriver åtkomst till FTPS

2.4 XML (Extensible Markup Language)

XML, Extensible Markup Language är ett allmängiltigt och utbyggbart märkspråk som används vid informationsdelning av dokument på internet. Märkspråk består av särskilda textkoder (kallas även för taggar eller element) som bestämmer struktur, utseende och betydelse på information i ett dokument

(Collin & Karlsson, 2001). Taggar gör att man kan se exakt vilken information som ska lagras i XML - dokument, dem möjliggör även att man kan definiera nästan vilken datastruktur som helst. XML är plattformsoberoende vilket gör att man kan bearbeta information oavsett operativsystem och maskinvaruplattform. Flexibiliteten är anledningen till att XML har blivit en av de mest använda teknikerna för utbyte av information över internet. En annan fördel är att applikationer kan bearbeta data direkt i XML - dokumentet, vilket stödjer automatisk dataöverföring mellan aktörer. XML har potential att öppna upp nya marknader och förenkla åtkomsten för aktörer genom att agera som ett standardiserat format för dataöverföringar (Collin & Karlsson, 2001; Ericsson, 2005). Nedan visas ett exempel på hur man kan lagra data i ett XML - dokument.

```
<?xml version="1.0"?>
<PRODUKT>
 <TYP>Mobiltelefon</TYP>
 <TILLVERKARE>Apple</TILLVERKARE>
 <MODELL>iPhone</MODELL>
 <LAGRINGSKAPACITET>64GB</LAGRINGSKAPACITET>
 <FÄRG>SVART</FÄRG>
 <SERIENUMMER>S01YUD67</SERIENUMMER>
 <IMEI>01248500-774091-5</IMEI>
</PRODUKT>
```

Taggar: TYP, TILLVERKARE, MODELL, LAGRINGSKAPACITET, FÄRG, SERIENUMMER, IMEI.

Figur 2.4 visar ett exempel på ett XML - dokument. Taggarna ovan gör det enkelt att förstå att dokumentet hanterar information om diverse produkter, i detta fallet en mobiltelefon av modellen iPhone.

3 Metod

I kapitlet presenterar vi den fallstudie som vi har utfört, samt de undersökningsmetoder som har används för att utvärdera och samla information för att svara på forskningsfrågan.

3.1 Fallstudie

Fallstudie är en beteckning som innebär att man undersöker ett mindre avgränsat område, vanligtvis en individ, grupp, organisation, process eller en situation. Vid fallstudier utgår man från ett helhetsperspektiv för att få en så övergripande bild av det aktuella fallet som möjligt, vilket kan öppna

upp möjligheten att diskutera generaliseringen av de resultat som man erhållit vid undersökningen (Patel & Davidson, 2011). En lyckad fallstudie kan ge en flerdimensionell bild av de mönster och relationer som förekommer i ett visst sammanhang. För att lyckas med det kan det vara nödvändigt att göra datainsamlingar av varierande karaktär och ur olika infallsvinklar. Ett förekommande problem med fallstudier är att tillförlitligheten kan ifrågasättas eftersom de personer och dokument som studien grundar sig på kan vara svår att kontrollera eller få tag på (Holme & Solvang, 2001).

Fallstudier kan tillämpas i explorativa och deskriptiva undersökningar. Explorativ undersökning innebär att det inte finns någon fast utgångspunkt för studien och forskaren söker efter vad som till en början inte visar på vad som är relevant, respektive irrelevant att utreda. Vanligast är att fallstudier används vid deskriptiva undersökningar, vilket innebär att det existerar ett problem eller frågeställning och där syftet är att utreda det enskilda fallet. Vid deskriptiva undersökningar förekommer ibland att generaliserbarheten av resultatet är begränsad eftersom man vid vissa fallstudier har inriktat sig för hårt mot att lösa ett specifikt problem (Holme & Solvang, 2001; Patel & Davidson, 2011).

3.1.1 Fallstudieobjekt

Vår fallstudie är en deskriptiv undersökning där vi har valt att betrakta en distributionsprocess av sekretessbelagd information på ett företag inom försvarsindustrin. Diadrom Systems AB har gett oss i uppgiften att se över möjligheten att skicka driftinformation om vapensystem mellan militära kunder och försvarsföretag över internet. Som tidigare nämnt har försvarsföretagets identitet anonymiserats på grund av sekretess- och säkerhetsskäl. Vi är medvetna om att anonymiseringen kan göra det svårt att kontrollera de källor som används för att få fram information om försvarsföretaget. Det ska dock inte påverka undersökningens resultat eftersom ambitionen med fallstudien är att generera generella riktlinjer för hur olika företag och organisationer på ett säkert sätt kan hantera skicka sekretessbelagd information över internet.

En gemensamt formulerad fråga blir utgångspunkten för vår fallstudie:

Hur kan information som utbyts mellan aktörer i geografiskt skilda områden kategoriseras och krypteras så att den kan transporteras över internet utan säkerhet- och integritetsbrister?

Utöver frågeställningen förhåller vi oss till en uppsättning krav som tagits fram i samarbete med Henrik Fagrell, VD på Diadrom. Kraven ligger till grund för hur lösningsförslagen ska tas fram och omfattar funktionella, allmän och tekniska villkor. Utformning av kraven har skett med åtanke på att lösningen ska kunna appliceras på situationer bortom det enskilda fallet.

3.1.1.1 Funktionella krav

- Försvarsföretaget ska kunna hantera olika säkerhetsnycklar för olika kunder.

- Försvarsföretaget ska kunna samma hantera basdata på olika sätt för olika kunder.

- Försvarsföretaget ska kunna flytta data via Internet med hög säkerhet.

- Försvarsföretaget ska kunna använda samma säkerhetskoncept för flera produktlinjer.

- Produktionen måste kunna producera flera olika produkter för flera kunder med olika säkerhetskoncept.

- Driften behöver kunna hantera flera kunder med olika säkerhetskoncept.

- Produktionen behöver kunna hantera flera kunder med olika säkerhetskoncept.

3.1.1.2 Allmänna krav

- Olika kunder får inte känna till andra kunders information.

- Driften måste kunna lagerlägga artiklar utan att på förhand veta vilken kund.

- Olika personer inom försvarsföretaget måste kunna hantera att viss data endast får hanteras av godkänd personal.

- Olika kunder får inte känna till andra kunders nycklar.

- Olika kunder får inte känna till andra kunders chiffer.

3.1.1.3 Tekniska krav

- Försvarsföretag och militära kunder ska inte vara beroende av att använda specifika operativsystem eller mjukvaruplattformar.

- Krypteringstekniken ska vara tillförlitlig och avancerad nog för att förhindra att obehöriga kan förstå information vid eventuella dataförluster som sker via transport över internet.

- Information ska skickas och tas emot via en dator med användaridentifiering och lösenord.

3.2 Datainsamlingsmetoder

I kapitlet beskrivs tillvägagångssättet för datainsamling för den här studien.

3.2.1 Litteraturstudier

Litteraturstudier används traditionellt för sådan information som finns nedtecknad eller tryckt, men på grund av den tekniska utvecklingen finns det idag flera alternativ för att bevara information. Vid litteraturstudier består datainsamlingen mestadels av vetenskapliga artiklar och avhandlingar, men det förekommer även att forskaren väljer att studera källor t.ex. ljud- och bilddokument, privata handlingar eller kortlivade dokument i egenskap av tidningar och information från internet. Ett hinder för den typen av källor är att det kan vara svårt att ta reda informations tillförlitlighet eftersom källförteckningar ofta saknas eller är bristande (Patel & Davidson, 2011).

I vår fallstudie har vi valt att använda oss av litteraturstudier som datainsamlingsmetod därför att det ansågs vara det mest rationella sättet att få fram relevant teori för problemet. Styrkan hos litteraturstudier ligger i att det ofta ger möjlighet att kritiskt granska undersökt material eftersom dokumenten i allmänhet anger referenser till det underlag som dem är baserade på. I studien var det viktigt för oss att kunna vara källkritiska av den anledningen att våra kunskaper inom området är begränsad.

Litteraturstudien gav oss en bättre förståelse för ämnesområdet såväl som de tekniker och arbetssätt som ligger till grund för den säkerhet som krävs för hantering av sekretessbelagd information. Resultatet av fallstudien grundar sig följaktligen helt eller delvis på de tolkningar som gjorts i samband med litteraturstudien, likaså de generella riktlinjer för distribution och hantering av känslig information.

3.2.2 Fokusgrupp

Fokusgrupp är en beteckning för en kvalitativ datainsamlingsmetod som i regel går ut på att diskutera ett särskilt fokus inom en grupp människor som har något gemensamt. Fokusgrupper kan tillämpas i de flesta skeden i en forskningsprocess och kan användas i flera olika syften, till exempel vid en explorativ inledning i ett okänt område, utvärderingar av diverse resultat eller för att generera och förklara teorier. Fokusgrupper ligger någonstans mellan ostrukturerade intervjuer och observationer, till skillnad från traditionella frågesamtal har metoden en benägenhet att starta mer ingående diskussioner (Hylander, 2001).

Skälet till att vi har valt att arbeta med fokusgrupper är för att vi anser att metoden är ett bra sätt för att utvärdera fallstudiens resultat. Det är viktigt för oss att få synpunkter av specialister på lösningar som vi har tagit fram med hjälp av litteraturstudier eftersom vår erfarenhet och kompetens inom området är begränsad.

Tanken var att vi vid ett par tillfällen skulle utvärdera lösningarna med försvarsföretaget. Detta för att ta reda på om det var fysiskt möjligt att implementera systemet i deras verksamhet i förhållande till dem riktlinjer och regler som gäller för hantering av sekretessbelagd information.

Materialet presenterades av olika skäl enbart vid ett tillfälle vilket gav oss en relativt fragmenterad utvärdering av lösningen för det specifika problem som diskuterats i fallstudien. För att få någon form av återkoppling diskuterades lösningarna vid upprepade tillfällen med Henrik Fagrell eftersom han har en inblick i hur försvarsföretaget arbetar.

3.2.3 Intervjuer

Utöver vår fokusgrupp har vi utfört ett antal mindre informella intervjuer med Henrik Fagrell, VD för Diadrom som har mångårig erfarenhet av att arbeta med försvarsföretaget och är väl insatt i hur deras arbetsätt ser ut och vilket säkerhetstänk som genomsyrar organisationen. Samtalen har bidragit med en central del av vår förståelse för försvarsföretagets nuvarande situation och arbetssätt.

4 Resultat

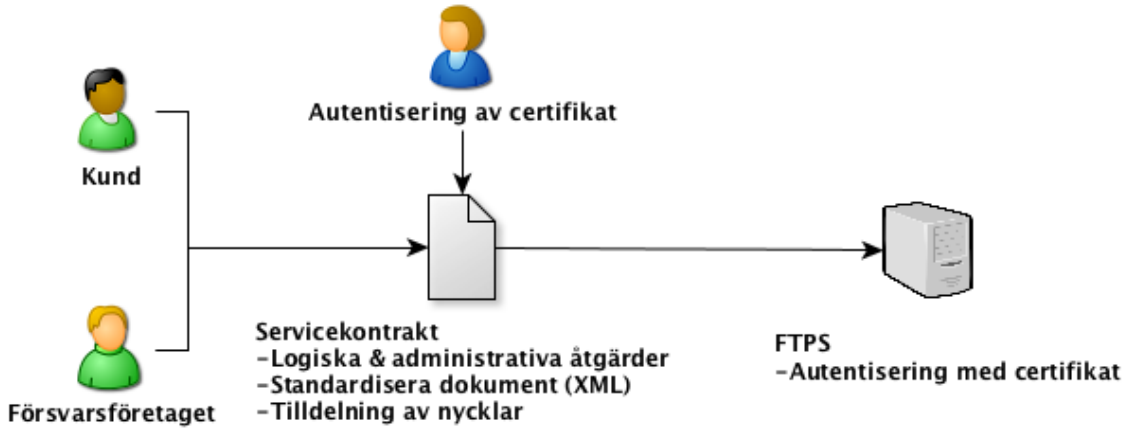
I kapitlet presenteras resultatet av fallstudien. Vi har valt att dela upp resultatet i två delar för att särskilja de generella riktlinjerna från det konkreta lösningsförslaget som relaterar till försvarsföretaget.

4.1 Lösningsförslag till fallstudien

I nuvarande situation väljer militära kunder att skicka driftinformation om vapensystem enligt traditionella försändelser via kurir och diplomatpost. För att kunna använda elektroniska alternativ för distribution av data är det viktigt att försvarsföretaget kan visa att dem klarar av att leverera en lösning med hög säkerhet och tillförlitlighet. Att skapa förtroende för en distributionsprocess kan ta lång tid och återkommande översikt. En bra början i arbetet skulle kunna vara genom att upprätthålla ett servicekontrakt mellan berörda parter. Servicekontraktet skulle förslagsvis kunna beskriva i vilken utsträckning som försvarsföretaget ska erbjuda service för det aktuella vapensystemet. Detta skulle kunna gagna båda parter eftersom det vid kontrakt införandet skulle kunna vara möjligt att komma överens om vilken information som kunden vill dela med sig av och därigenom fastställa de krav som ställs på säkerhet. Med kontrakt införandet som utgångspunkt kan det vara lättare att komma överens om de logiska och administrativa åtgärder som krävs för att uppnå den säkerhet som krävs i

sammanhanget. Dem administrativa åtgärderna skulle i fallet kunna bestå av att fastställa värdet av information och klassificera den så att man kan avgöra hur information ska hanteras och av vilka personer. Utifrån denna ståndpunkt är det lättare att föreslå vilka logiska åtgärder som passar för den specifika kunden. Med logiska åtgärder menar vi dem tekniska alternativ som kan anpassas efter situationen, såsom kryptering av data, filöverföringsprotokoll- och standarder. RSA är en långsam krypteringsalgoritm och har därför valts bort i lösningsförslaget. Smart card har även valts bort då detta kräver ytterligare hårdvara för att kunna användas (Hansson, 2009; Frank, 2011; Ehsas, 2011).

Figur 4.1 illustrerar hur denna arbetsprocess hade kunnat se ut.



Figur 4.1 beskriver en möjlig arbetsprocess för att åstadkomma elektronisk distribution av känslig data över internet

4.1.1 PKI (Public Key Infrastructure) ett alternativ för att certifiera nycklar

PKI, Public Key Infrastructure ger användare möjlighet att distribuera asymmetriskt krypterad (se *asymmetrisk kryptering* kapitel *2.2.1*) information över osäkra nätverk. PKI kan vara ett lämpligt sätt för att skapa förtroende mellan parterna genom att fastställa en tillförlitlig kontakt som ansvarar för att verifiera att krypterad information kommer från en användare med giltigt certifikat.

4.1.2 XML (Extensible Markup Language) ett alternativ för datastruktur

XML, Extensible Markup Language kan vara en bra filtyp att använda för att lagra information om driftparametrar under distributionsprocessen. Främst för att XML är plattformsoberoende och bidrar till att militära kunder och försvarsföretaget inte behöver förhålla sig till ett specifikt operativsystem eller mjukvaruplattform. Men även av den anledning att XML är enkelt att anpassa efter den information som kunden väljer att dela med sig av till försvarsföretaget. För att uppnå ytterligare säkerhet skulle parterna komma överens om att döpa taggar till sådant som inte beskriver innehållets innebörd. På så vis är det

svårt att tyda vad innehållet betyder vid eventuella dataförluster. Figur 4.2.3 och 4.2.3 visar hur vi har tänkt med vilseledande taggar.

```
<?xml version="1.0"?>
<VAPENSYSTEM>
 <NATION>Sverige</NATION>
 <DRIFTTIMMAR>85</DRIFTTIMMAR>
 <SKJUTNINGAR>32</SKJUTNINGAR>
 <KALIBER>50</KALIBER>
</VAPENSYSTEM>
```

Figur 4.3.2 visar ett exempel på ursprungsinformation om ett vapensystem

```
<?xml version="1.0"?>
<PERSON>
 <URSPRUNG>Sverige</URSPRUNG>
 <VIKT>85</VIKT>
 <ÅLDER>32</ÅLDER>
 <SKOSTORLEK>50</SKOSTORLEK>
</PERSON>
```

Figur 4.3.2 visar ett exempel på vilseledande taggar med information om vapensystem

Vilseledande förklaringar av taggar skulle kunna anpassas efter vad som i situationen är lämpligast. Liknande lösning skulle kunna appliceras i datalagring, men istället för taggar använda sig av vilseledande tabellnamn som refererar till de värden som efterfrågas. Dock är datalagring något som vi i denna uppsatsen har valt att inte diskutera.

4.1.3 FTPS (SSL File Transfer Protocol) ett alternativt filöverföringsprotokoll

FTPS, SSL File Transfer Protocol kan vara ett bra alternativ för att sprida och lagra information om driftparametrar. Främst för att FTPS är plattformsoberoende och bidrar till att militära kunder och försvarsföretaget inte behöver förhålla sig till ett specifikt operativsystem eller mjukvaruplattform. Men även av den anledningen att FTPS kan verifiera att försvarsföretaget eller en militär kund med PKI kan certifiera sig för att få åtkomst till information (se *Certifiering av nycklar med PKI* kapitel 2.2.1.1)

4.2 Generella riktlinjer för att uppnå säker distribution av data

Enligt Hallén och Larsson är de administrativa åtgärderna den process som anses vara den mest komplexa. Riktlinjerna är framtagna med hjälp av våra egna erfarenheter och den information som vi tagit till vara från vår litteraturstudie.

- För att uppnå den säkerhet man strävar efter i en process eller situation är det viktigt att ha en strategi för hur man ska fördela arbetet.

- Ett bra alternativ kan vara att börja med att skapa en förståelse för informations värde och betydelse för organisationen, detta görs enklast genom en klassificeringsprocess.

- Skapa en förebyggande strategi som går ut på att förhindra att icke önskvärda situationer uppstår.

- Skapa en begränsad strategi som går ut på att minska skadan i organisationen vid ett eventuellt intrång.

- Skapa en strategi för rapportering som går ut på att varna eller uppmärksamma organisationen vid intrång.

Med dessa administrativa åtgärder som utgångspunkt underlättas arbetet med att ta fram en teknisk motsvarighet till problemet som man vill lösa.

- Skapa tekniska förutsättningar för att uppnå den säkerhet som informationen kräver.

- Ett bra alternativ kan vara att börja med att se över befintliga lösningar för kryptering, lagring och distribution av data på internet.

- Sträva efter att välja plattformsoberoende lösningar eftersom det tillåter verksamheten att anpassa lösningen efter de dynamiska förhållanden som vanligtvis råder inom organisationer.

5 Resultatanalys

Resultatet av fallstudien hade troligtvis kunnat se annorlunda ut om vi hade haft en tätare dialog med försvarsföretaget med anledning av att vi inte fått tillräckligt konkret feedback om de lösningsförslag som presenterades ovan. Trots detta tror inte vi att det kommer påverka hur vi har valt att utforma dem generella riktlinjer som redovisats i stycke ovan, detta eftersom vi anser att svårigheten i att finna säkra sätt att distribuera information över internet inte ligger i den teknik som används vid förförandet.

6 Slutsats

Informationssäkerhet är ett ämne med varierande karaktär och med många infallsvinklar. Det är svårt att säga exakt vad som menas med begreppet eftersom innebörden varierar beroende på vilket sammanhang som ämnet diskuteras. Informationssäkerhet kan därmed ha olika betydelse för olika företag och organisationer. Utifrån detta resonemang har vi kommit fram till svar på följande fråga:

"Hur kan information som utbyts mellan aktörer i geografiskt skilda områden kategoriseras och krypteras så att den kan transporteras över internet utan säkerhet- och integritetsbrister?"

För att lyckas med ett säkerhetsarbete omkring en process, situation eller något så heltäckande som en organisation är det viktigt att ta reda på vad man vill åstadkomma för att därifrån skapa en strategi för att nå det resultat som man eftersträvar. Ett bra sätt att påbörja arbetet är genom att se över vilken information som flödar genom organisationen och försöka ge den ett värde via en klassificeringsprocess. Genom att ha en förståelse för informations värde är det lättare att sätta upp generella riktlinjer för hur den bör hanteras av olika personer och system.

I nuläget är informationsteknologi ett såpass utvecklat område så att den inte anses som ett hinder för att möjliggöra säker lagring, distribution eller bearbetning av känslig data. Den största utmaningen är istället de administrativa åtgärder som krävs för att få en förståelse för hur information ska hanteras innan- och utanför organisationen. Genom att förstå värdet på informationen är det lättare att föreslå vilka tekniska alternativ som kan användas för att uppnå önskat resultat. Det finns därför inget distinkt svar på hur man kan uppnå säkerhet i en distributionsprocess eftersom det beror på så mycket annat än de tekniska förutsättningar som finns.

7 Referenser

Litteratur

Frank, C. (2011). *Kryptografi - en introduktion,* Studentlitteratur, Lund, Sverige.

Holme, I. Solvang, B. (2001) *Forskningsmetodik -Om kvalitativa och kvantitativa metoder*, Studentlitteratur, Lund, Sverige.

Pardon - McCarthy, T. Risch, T. (2005) *Databasteknik,* Studentlitteratur, Lund, Sverige.

Patel, R. Davidson, B. (2011). *Forskningsmetodikens grunder,* Studentlitteratur, Lund, Sverige.

Källor på internet

Andersson, J. (2002) *Rekommendationer för införande av public key infrastructure.*

Botrakoff, M. (2009). *Secure File Transfer Protocol - User Guide.*

Broman, F. Lindgren, D. (2004). *Effektiv hantering av information.*

Collin, H. Karlsson, V. (2001). *EDI eller ebXML? - för automatisering av affärsprocesser.*
Ehsas, N. (2011). *Introduktion till krypteringsmetoderna RSA och Merkle-Hellman.*

Ericsson, M. (2005). *Utvärdering av säkerhetsspecifikationer för XML.*

Försvarshögskolan. (2013-04-20). *Hantering av sekretessbelagd information* .

Hallén, K. Larsson, N. (2010). *Informationsklassificering - ett styrdokument för klassificering av informationssystem.*

Hylander, I. (2001). *Fokusgrupper som kvalitativ datainsamlingsmetod.*

Myndigheten för samhällskydd och beredskap. (2013-05-14). *Modell för klassificering av information.*

Palmér, H. & Vickberg, A. (2011). *Hur påverkas partnerskap när information är sekretessbelagd?: En studie om hur sekretessbelagd information påverkar kommunikationen inom partnerskap mellan Saab Aeronautics och deras partners och vad det får för konsekvenser*

för partnerskapet.

Seshadri, A. Perrig, A. Van Doorn, L. (2013-04-24). *Using Software-based Attestation for Verifying Embedded Systems in Cars.*

Westin, A. (2011). *Klusterbaserad dataspridning med FTP/FXP*.

Botrakoff, M. (2009). *Secure File Transfer Protocol - User Guide.*

Pettersson, F. (2008). *File transfer protocol (FTP) - Problem och lösningar.*

Muntliga referenser

Fagrell, H. (2013). VD Diadrom, Göteborg, Sverige.