Datacentrerad säkerhet

Amund Gudmundson Hunstad, Lars Westerdahl

FOI-R--4865--SE

December 2019

FOI

Amund Gudmundson Hunstad, Lars Westerdahl

Datacentrerad säkerhet

Titel	Datacentrerad säkerhet
Title	Data-centric security
Rapportnr/Report no	FOI-R--4865--SE
Månad/Month	December
Utgivningsår/Year	2019
Antal sidor/Pages	36
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	Informationssäkerhet
FoT-område	Operationer i cyberdomäner
Projektnr/Project no	E72777
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Bild/Cover: Caroline Bildsten, FOI

Sammanfattning

Informationssäkerhet är ett brett område. För informationssystem har informationssäkerhetsarbetet i praktisk mening främst fokuserat på att skydda de IT-system där informationen lagras samt skydda informationen när den transporteras mellan dessa system. Denna ansats kan idag upplevas som begränsande då behovet av en snabb tillgång till information har ökat, dels mellan egna system, dels mellan system från andra säkerhetsdomäner. Behovet av att centralt kunna styra vilken information som kan delas med vem, vare sig det är konsumenter av information inom den egna verksamheten eller om det är en partner i en koalition, har ökat med åren.

Datacentrerad säkerhet (DCS) är ett koncept med fokus på *vad* som ska skyddas i första hand och inte *var* informationen finns. Centrala principer för DCS är en *central säkerhetsförvaltningsfunktion*, *sömlöst skydd*, *automatiserade säkerhetsprocesser* samt *anpassningsförmåga*.

I denna rapport beskrivs och relateras DCS till utveckling inom närliggande områden som attributbaserad åtkomstkontroll och attributbaserad kryptering samt utvecklingsprojekt och forskning från andra länder. Målet med rapporten är att beskriva mognadsgraden för DCS-lösningar i syfte att stödja Försvarsmaktens arbete inom exempelvis *Federated Mission Networking* (FMN).

Nyckelord: Datacentrerad säkerhet, objektbaserad säkerhet, koalitioner, interoperabilitet, säkerhetsdomäner

Summary

Information security is a wide field of study. For information systems, information security efforts has in the practical sense mainly focused on protecting IT systems that store information and the protection of information when it is transported between these systems. This approach can today be seen as limiting because the need for quick access to information has increased, partly internally between one's own systems and partly between systems from different security domains. The need to control what information can be shared centrally and with whom, whether it be consumers of information within the organization's own operations or a partner in a coalition, has increased over the years.

Data-centric security (DCS) is a concept that primarily focuses on *what* should be protected and not *where* the information is stored. Key principles for DCS are a *Centralized control*, *Gapless Protection*, *Automation* and *Adaptability*.

In this report, the concept of DCS is described and related to development in fields such as Attribute-Based Access Control and Attribute-Based Encryption, as well as development projects and research from other nations. The goal of this report is to describe the degree of maturity for DCS solutions with the goal of supporting the Swedish Armed Forces' work with, for example, Federated Mission Networking (FMN).

Keywords: Data-centric security, object based security, coalitions, interoperability, security domains

Innehållsförteckning

1. Inledning

Interoperabilitet, det vill säga förmågan att samverka med andra, är central för Försvarsmakten. Under de senaste decennierna har Försvarsmakten deltagit i ett flertal internationella koalitioner, vilka alla satt interoperabiliteten på prov. På senare tid har även interoperabilitet med andra nationer i närområdet fått betydelse genom bilaterala samarbeten och värdlandsavtal.

Förmågan till interoperabilitet kan definieras och beskrivas på flera nivåer, från systemteknisk nivå till gemensamma begrepp och terminologi för den verksamhet som bedrivs. Den tekniska nivån kan brytas ner ytterligare i delnivåer, vilka omfattar allt från standarder för informationsutbyte mellan nationer till att enskilda enheter kan kommunicera direkt med varandra under pågående uppdrag. Det senare har varit svårt att uppnå till och med över truppslagsgränserna inom Försvarsmakten, vilket tydligt pekar på de stora utmaningar som finns inom området. En ytterligare försvårande omständighet är att större enheter ofta sätts samman av mindre enheter som inte tidigare samarbetat. Då kan svårigheter i kommunikationen mellan respektive enhets tekniska system uppstå även på nationell nivå.

Inom området informationssäkerhet har funktioner för att uppnå konfidentialitet, riktighet och tillgänglighet varit normen. Av dessa har konfidentialitet varit den egenskap som fått mest fokus, ibland på bekostnad av de övriga två. Efter hand som användandet av informationssystem ökat och därmed även graden av automation, har behovet av automatiserade säkerhetslösningar också ökat. Det är inte längre realistiskt med manuell informationshantering över domängränser och det finns ett större behov av att kunna dela information mer effektivt. Ytterligare en aspekt av dagens användning av informationssystem är den grad av mobilitet som präglar användningen av dessa system. Det gör att information behöver vara mer tillgänglig än tidigare men även att dynamiken kring säkerhetsegenskaperna förändras. Det finns därför behov av att se över de metoder som används för att hantera åtkomstkontroll till information i informationssystemen. Istället för att koppla åtkomstbeslut till vem som är behörig till vilket system, finns det ett behov av att fatta detta beslut på vad informationen innehåller och under vilka förutsättningar som åtkomsten begärs.

Datacentrerad säkerhet (DCS), är ett högnivåbegrepp för säkerhetsåtgärder med fokus mot innehållet i informationen. Projekt för utveckling av datacentrerade lösningar har drivits i flera år av olika nationer, standardiseringsorgan och systemutvecklare. Lösningarna har dock divergerat i och med att det saknas en generell definition av konceptet. Försvarsmakten har önskat att projektet IT-säkerhetsmetoder ger en översikt av utvecklingen på detta område. I den här

rapporten presenteras därför vad en datacentrerad säkerhetslösning[1] innebär och vilka tekniker som stödjer detta i dagsläget. Studien har genomförts inom ramen för Försvarsmaktens samlingsbeställning inom forskning- och teknikutveckling (FoT), i projektet IT-säkerhetsmetoder som ingår i FoT-området Operationer i cyberdomänen.

1.1 Syfte och mål

Syftet med uppdraget är att stödja Försvarsmakten i deras arbete med en säkrare informationshantering. Målet med rapporten är att presentera en omvärlds-bevakning av området datacentrerad säkerhet.

1.2 Avgränsningar

De tekniker som undersöks har begränsats till sådana som tillhör en tjänste-baserad arkitektur[2]. Motivet till detta är dels att en tjänstebaserad arkitektur medför en mer generisk ansats för att uppnå informationssäkerhet, dels att de lösningsförslag som tidigare har studerats vid FOI också har varit tjänste-baserade lösningar.[3]

1.3 Rapportstruktur

I kapitel 2 presenteras en bakgrund till ämnet och tidigare arbeten, både inom Totalförsvarets forskningsinstitut (FOI) och från andra källor. Kapitel 3 presenterar en omvärldsanalys av kända tekniker och initiativ inom området. Resultat från de inledande kapitlen analyseras i kapitel 4 och diskuteras i kapitel 5.

[1] Eng. Data Centric Security (DCS).

[2] Eng. Service-Oriented Architecture (SOA)

[3] Se exempelvis Westerdahl, L., Hunstad, A.G. & Mörnestedt, F. (2014b).

2. Grundläggande begrepp

I detta kapitel förklaras på en övergripande nivå terminologi inom området datacentrerad säkerhet och närliggande forskningsområden. Vad som utgör allmänna tekniska utmaningar inom datacentrerad säkerhet samt dess tillämpningsområden ingår också i denna redogörelse.

2.1 Datacentrerad säkerhet

Datacentrerad säkerhet är ett koncept, inte en existerande teknisk tillämpning. I litteraturen om DCS är i dagsläget fokus på önskvärda egenskaper som DCS bör ha. Vad som primärt särskiljer datacentrerad säkerhet från andra säkerhetstekniker är ett fokus på *vad* som är i behov av att skyddas, mera än *var* det befinner sig (PKWARE 2019). Med fokus på var data befinner sig kan säkerhetsutmaningar uppstå om data förflyttas från en server till en annan eller om data passerar ett visst nätverk eller en viss zon.

IT-system utgår i sin uppbyggnad till betydande grad från tekniska förutsättningar, vilket typiskt innebär en arkitektur som tillhandahåller effektiv datakommunikation i ett nätverk. Som en förenkling benämns detta här som en nätverkscentrerad lösning.

Nätverkscentrerade lösningar har normalt ett fokus på att identifiera, kategorisera och hantera datatrafik, vilket förenklat innebär ett perspektiv av att hålla reda på *var* data befinner sig. Exempelvis används brandväggar och intrångsdetekteringssystem för att sålla bort oönskad trafik, som kan överbelasta eller innehålla angrepp. Här kan ett förtydligande behövas, nätverkscentrerade lösningar är viktiga och nödvändiga, men de täcker inte med självklarhet alla behov relaterade till perspektivet *vad* som är i behov att skyddas. Vad som behöver skyddas beror även på verksamhetsmässiga och organisatoriska förutsättningar och hur data skapas, förvaltas och används.

För kritiska och känsliga data kan det vara särskilt kritiskt var de befinner sig, exempelvis om de är inom eller utanför sin vanliga säkerhetsdomän. SANS (2019) beskriver DCS som tillägg till nätverksorienterade lösningar, för att skydda verksamheters och organisationers särskilt kritiska eller känsliga data. DCS innebär med andra ord ur detta perspektiv att noggrant beakta *vad* som är centralt och viktigt för verksamheten eller organisationen. För att förvalta och hantera data på bästa möjliga sätt krävs kännedom om hur åtkomst till och användning av data sker, såväl i enkla filtjänster som i komplexa webbtjänster.

DCS har fokus på innehåll och kontext, mera än på trafik. Med andra ord eftersträvar DCS att identifiera vad som är särskilt kritiska data för en viss organisation i ett visst sammanhang och att sedan skydda dessa med särskilt

anpassade skyddsmekanismer. Patientjournaler, styrsystemsdata avseende kritiska infrastruktur eller kommunikationsdata inom en koalition är exempel på data som kräver skydd på annan nivå än vad exempelvis publika data på en webbserver kräver. Inom DCS-konceptet är en bärande idé att dessa skyddsmekanismer ska tillämpas helt automatiskt, vilket nuvarande lösningar inte nödvändigtvis gör.

Verksamheter och organisationer använder i ökande omfattning molnteknologi och mobila lösningar, vilka medför att tidigare nätverkscentrerade säkerhetslösningar inte räcker till (Oltsik 2015) och att gränsen för den egna säkerhetsdomänen tenderar att bli otydlig (O'Connor 2018). Känsliga data riskerar att vara lagrade på flera ställen och med otillräcklig kontroll, samtidigt som kontrollmekanismer till betydande grad fortfarande är manuella. Gartner (2014) pekar på att utvecklingen kring *Big Data* och molnlagring innebär att organisationers säkerhetspolicyer och säkerhetsprocesser inte längre är tillräckliga. Detta eftersom utgångspunkten för dessa policyer fortfarande är den egna säkerhetsdomänen och egna, kontrollerbara system och nätverk. När data till betydande grad är placerade på andra ställen, får säkerhetsutmaningarna en annorlunda karaktär än vad policyer och processer har utvecklats för. Även säkerhetskopiering kan medföra att data hamnar på ställen utanför en nätverkscentrerad lösnings kontroll, något som ofta policyer och processer inte tillräckligt tydligt har anpassats för. DCS omfattar koncept och metoder för att hantera ovan beskrivna utvecklingstendenser.

Datacentrerad säkerhet har även potential att bidra i scenarion där omfattande datamängder hanteras mellan olika organisationer för att lösa gemensamma uppdrag. Koalitioner behöver typiskt bygga gemensamma kommunikationslösningar för att lösa koalitionsuppdraget. Respektive koalitionspartner tillhandahåller vanligtvis inte åtkomst till eget nätverk för andra koalitionspartners. I sådana sammanhang är i växande omfattning operationell, procedurell och teknisk interoperabilitet kritiska att uppnå. Militära koalitioners övergripande behov av datainteroperabilitet berörs av Harrison (2012).

Tillämpning av DCS kräver automatiserade processer som identifierar skyddsvärda data och som effektivt hanterar dessa på adekvata och relevanta sätt. Nämnda automatiserade processer innebär att bedömningar av skyddsbehovet inte längre är individberoende. Vidare krävs sofistikerade mjukvaruagenter och en centraliserad säkerhetsförvaltningsfunktion som definierar vad som utgör adekvat och relevant skydd för respektive datakategori och användningsfall. Dessutom behöver ramar specificeras inom vilka den centraliserade förvaltningsfunktionen kan agera och besluta, vilket får till följd att policyer måste formuleras.

Avsikten med DCS är att skyddet för data kvarstår oavsett var data befinner sig, även utanför en organisations nätverk och system. För att definiera vilken säkerhetsnivå som krävs, är välformulerade och täckande policyer kritiska. I dessa beskrivs vilken hantering av olika datakategorier som är tillbörlig respektive inte tillbörlig i olika kontexter. Likaså är nämnda automatiserade säkerhetsprocesser kritiska för att för olika enskilda datauppsättningar kunna realisera vad policyerna i generella termer beskriver. De automatiserade säkerhetsprocesserna övervakar dataflöde inom och mellan organisationer för att kontinuerligt kunna tillämpa adekvat och relevant skydd för känsliga data (O'Connor 2018; PKWARE 2019).

I en och samma organisation kan ett antal policyer, datakategorier och användningsfall existera, utgående från olika identifierade behovsbilder. Noggrann genomgång behövs av policyer, datakategorier och användningsfall för att säkra att de samverkar på bästa möjliga sätt. Behov kan rent av vara motstridiga, vilket kan medföra behov av förhandling och icke minst risk-bedömningar där aktuella datakategorier bedöms relativt användningsfall, associerade risker, säkerhetsåtgärder, legala förutsättningar, standarder etcetera (O'Connor 2018; PKWARE 2019).

I PKWARE (2019) beskrivs sammanfattande några centrala principer för DCS:

- central säkerhetsförvaltningsfunktion
- sömlöst skydd
- automatiserade säkerhetsprocesser
- anpassningsförmåga.

Denna lista gör inte anspråk på att vara komplett, men den sammanfattar vad de flesta verkar vara överens om som en beskrivning av DCS. En central säkerhets-förvaltningsfunktion tillser att data skyddas i överensstämmelse med organisationens säkerhetspolicyer. Likaså tillser den centrala funktionen att data i överensstämmelse med policyer är tillgängliga för behörig användning. Särskilt viktigt är hantering av kritiska och känsliga data. Sömlöst skydd[4] använder PKWARE (2019) som beskrivning av skydd för att säkra data även när de är utanför sin typiska, vanliga säkerhetsdomän eller plattform. Automatiserade säkerhetsprocesser är av särskild vikt i lägen där data flyttar sig mellan domäner och plattformar. Dataflöden är ofta av en sådan omfattning att det enda rimliga alternativet är automatiska processer, ty manuella blir otillräckliga. Anpassningsbarhet är av vikt för att över tid och sammanhang effektivt förvalta olika kravuppsättningar, datakategorier, policyer, kontexter och användningsfall.

[4] Eng. Gapless protection

Policyer är ur perspektivet i PKWARE (2019) av vikt för att klargöra krav, skyldigheter och behov som förväntas vara uppfyllda. Krav, skyldigheter och behov kan härröra från olika aktörer, som exempelvis säkerhetsrevision, myndigheter, avnämare eller styrande nivåer inom organisationen. Vidare är policyer viktiga för att klargöra avvägningar kring identifiering och hantering av kritiska och känsliga data.

För att uppnå och bibehålla ovan listade centrala principer för DCS diskuterar PKWARE (2019) på en övergripande nivå viktiga förmågor som behövs. En del av dessa förmågor är tekniska till sin natur. Bland annat rör det sig om adekvat och relevant kryptering respektive stöd för policyförvaltning. Vidare accentueras behov av olika funktioner för att detektera och hantera kritiska och känsliga data. Det rör sig om övervakning av dataflöden, klassificering med hjälp av beskrivande metadata och datamaskering. Slutligen poängteras också behov av uppföljande förmågor som rapportering och säkerhetsrevision.

2.2 Objektbaserad säkerhet

Vid FOI har till DCS näraliggande forskningsområden studerats under benämningen objektbaserad säkerhet. Benämningen är FOI:s egen. Denna verksamhet genomfördes inom FoT-projektverksamhet i samband med en förstudie 2007 och i två separata FoT-projekt under åren 2009–2014. (Hunstad, Gustafsson, Karlzén, Mörnestedt & Westerdahl 2012; Westerdahl, Hunstad & Mörnestedt 2014b)

2.2.1 Visionen om objektbaserad säkerhet

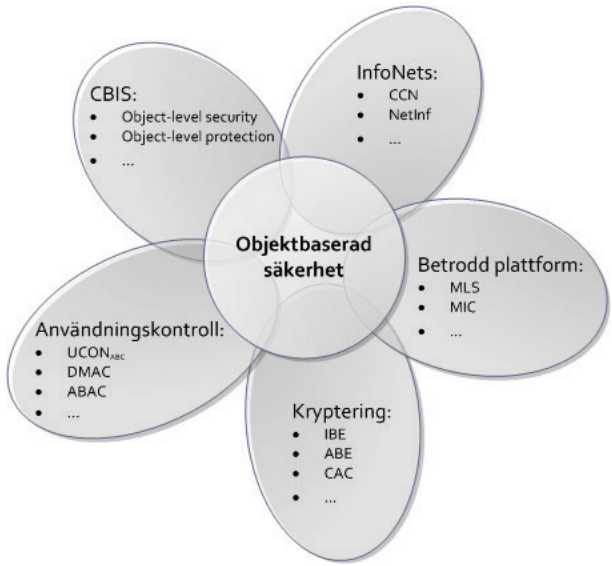
Objektbaserad säkerhet (OBS) innebär att säkerhetsfunktionalitet knyts direkt till informationsobjektet, för att möjliggöra att det bär med sig nödvändigt skydd utanför nuvarande informationssystem istället för att vara beroende av en skyddande zon (Westerdahl, Hunstad & Mörnestedt 2014b). Att nå ett höggradigt skydd utanför en skyddande zon utgör en betydande och komplex utmaning, vilket medför att detta omnämns som visionen om objektbaserad säkerhet. För att nå denna vision finns ett behov av att uppnå följande mål:

- finmaskig policy för dynamisk informationsåtkomst och informationshantering
- säker tredjepartslagring av information utanför den egna zonen
- upprätthållande av åtkomstkontroll även i offlineläge.

Om visionen uppfylls skulle det innebära att information i större grad kan spridas mera öppet och även utanför en organisations eller verksamhets normala skyddande zon, utan att göra avkall på säkerheten.

2.2.2 Relaterade forskningsområden

I samband med en litteraturstudie identifierades en handfull olika forsknings-områden relaterade till OBS som har potential att bidra till att uppfylla visionen om OBS (Hunstad, Gustafsson, Karlzén, Mörnestedt & Westerdahl 2012; Westerdahl, Hunstad & Mörnestedt 2014b).



Figur 1 Forskningsområden relaterade till objektbaserad säkerhet[5]

Figur 1 visar de olika forskningsområden som identifierades 2012 inom relaterad FoT-projektverksamhet. De övergripande kategorierna fokuserar på:

- Användningskontroll: Kontinuerlig autentisering och auktorisering, det vill säga inte endast vid öppnande av informationsobjekt. Attribute-Based Access Control (ABAC) är en i sammanhanget intressant lösning.
- Betrodd plattform: Säkrad informationshantering inom enskilda system.
- Informationsfokuserade nätverk (InfoNets): Säkrad informations-hantering inom nätverk.

[5] Figur från Hunstad, Gustafsson, Karlzén, Mörnestedt och Westerdahl (2012).

- Content Based Information Security: Säkrad informationshantering mellan säkerhetsdomäner.
- Kryptering: Auktorisering oberoende av var data befinner sig, även utanför egna kontrollerade system och nätverk. Attribute-Based Encryption (ABE) är en i sammanhangen intressant lösning.

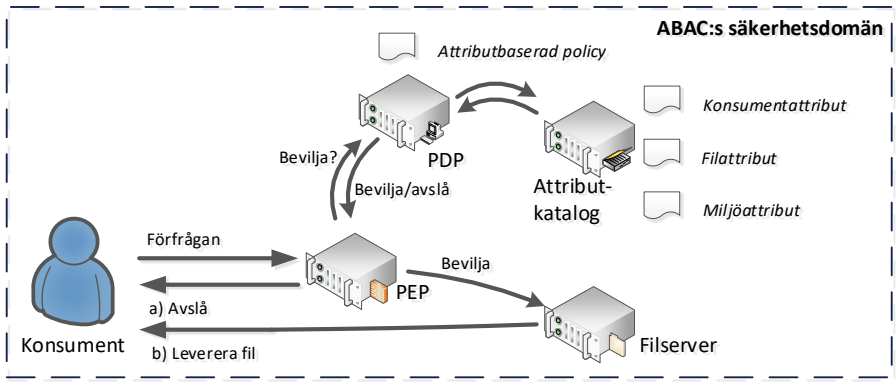
ABAC och ABE bedöms vara lösningar av särskilt intresse att granska inom ramen för OBS-visionen. ABE ligger närmast OBS-visionens huvudtanke, men bedöms i dagsläget huvudsakligen ha studerats inom akademisk forskning och har inte så här långt rönt större tillämpningsintresse utanför akademin. ABAC-tillämpningar existerar i dagsläget (Westerdahl, Hunstad & Mörnestedt 2014b).

3. Tekniker för DCS

DCS är ett koncept för att beskriva en miljö där information bedöms efter dess innehåll och värde, snarare än efter var den är lagrad. Eftersom det är ett koncept så finns det inte någon given teknisk implementation som uppfyller DCS målsättning till fullo. I detta kapitel presenteras därför ett urval tekniker som kan utgöra en grund för att implementera DCS. Vidare ges även en kort överblick över initiativ från andra länder och organisationer.

3.1 Attributbaserad åtkomstkontroll

Attributbaserad åtkomstkontroll[6] syftar till att skapa en mer detaljerad åtkomstkontroll till information jämfört med vad traditionell identitets- eller rollbaserad åtkomstkontroll erbjuder. Detta åstadkoms genom att åtkomstbeslut fattas baserat på en policy för informationen och dess användning. De parametrar (attribut) som bedöms är beskrivningar av den användare som vill få åtkomst till informationen, omgivande miljövariabler, samt egenskaper hos informationen. Figur 2 ger en övergripande bild av ett attributbaserat åtkomstsystem.



Figur 2 Översiktbild av attributbaserad åtkomstkontroll[7]

Den attributbaserade åtkomstprocessen börjar med att en konsument (den som vill få åtkomst) begär åtkomst till en fil på en filserver. På filservern finns en funktion som fångar upp förfrågan och skickar förfrågan vidare för

[6] Eng. Attribute-Based Access Control, ABAC

[7] Figur från Westerdahl, Hunstad och Mörnestedt (2014a).

policygranskning. Den funktion som fångar upp förfrågan benämns oftast som en *Policy Enforcing Point* (PEP). PEP:en skickar förfrågan till en *Policy Decision Point* (PDP) där attribut från konsumenten, filen och miljövariabler ställs mot en policy. Om policyn accepterar attributen skickas ett godkännande tillbaka till PEP:en, vilken i sin tur beviljar åtkomst till den fil som efterfrågades.

De attribut som är relevanta att använda kan skilja från organisation till organisation och från verksamhet till verksamhet. Då det inte finns en uppsättning givna attribut för dessa, skapas attributen istället så att de reflekterar organisationens bedömningskriterier. Det samma gäller för informationen (filen), där egenskaper hos innehållet beskrivs så att en policy kan användas för att fatta ett åtkomstbeslut. Miljöfaktorer är sådana variabler av momentan karaktär, exempelvis aktuell tid och varifrån förfrågan kommer, men kan även inkludera egenskaper avseende skyddsnivå.

I och med att det finns en central policy som styr åtkomst kan denna ändras över tid beroende på hur informationen värderas. Jämfört med en traditionell identitetsbaserad åtkomstkontroll där en användare alltid är lika behörig, oavsett från vilken fysisk plats eller system åtkomsten efterfrågas, ger attributbaserad åtkomstkontroll en högre grad av detaljnivå i åtkomstbesluten.

Den nod (PEP) som fångar upp en förfrågan behöver inte nödvändigtvis vara placerad på den server som den efterfrågade informationen finns på. Attributbaserad åtkomstkontroll stödjer en tjänstebaserad modell, där en PEP exempelvis kan vara placerad i en gateway för att avgöra vilken information som får lämna nätverket.

Attributbaserad åtkomstkontroll finns definierad i OASIS standarden *eXtensible Access Control Markup Language* (XACML) (OASIS 2013).

3.2 Attributbaserad kryptering

Kryptering används för att dölja innehållet i en fil för obehöriga läsare. Moderna krypteringsmetoder kan klassas in som symmetriska eller asymmetriska metoder. Inom symmetrisk kryptering delar avsändare och mottagare samma nyckel för kryptering och dekryptering. Det innebär att alla som har tillgång till denna nyckel kan skapa och läsa information med stöd av denna nyckel. Det innebär också att nyckeln kan användas i en grupp där alla delar denna nyckel, vilken då blir en gemensam hemlig nyckel. Fördelen med symmetrisk kryptering är att det är en snabb och effektiv metod samt, förutsatt att nyckeln inte avslöjas och är tillräckligt lång, bedöms som en säker metod. Nackdelen är just att om nyckeln avslöjas så blir allt som nyckeln använts till tillgängligt för den som har avslöjat nyckeln. En annan nackdel är att det inte går att avgöra vem som

krypterat ett meddelande i och med att alla använder samma nyckel. Asymmetrisk kryptering använder två nycklar: en publik nyckel som används för att kryptera ett meddelande och en hemlig nyckel som mottagaren använder för att dekryptera meddelandet. Detta innebär att den publika nyckeln kan spridas till vem som helst som vill kommunicera med innehavaren av den hemliga nyckeln men det är bara innehavaren av den hemliga nyckeln som kan läsa meddelandet. Om ett certifikat kopplas till den publika nyckeln, det vill säga en spårbar koppling till ägaren av motsvarande hemlig nyckel, kan man med hög säkerhet säkerhetsställa vem som man ska kommunicera med. Nackdelen med asymmetrisk kryptering är att den är mer beräkningskrävande och därmed långsam. Detta kompenseras genom att asymmetriska metoder och certifikat används för identifiering men att man krypterar en slumpmässig symmetrisk nyckel vilken endast kommer att användas för kryptering av den aktuella konversationen. Den symmetriska nyckeln blir då en sessionsnyckel utan koppling till andra konversationer.

Gemensamt för traditionella symmetriska och asymmetriska metoder är att nycklar måste distribueras i förväg, antingen direkt till mottagarna eller till en certifikattjänst när det gäller asymmetriska nycklar. Mottagarna av meddelanden är dessutom kända: för symmetriska genom kontrollerad spridning av den hemliga nyckeln och för asymmetriska genom det certifikat som är kopplat till den publika nyckeln.

Det finns dock situationer där mottagarna av ett meddelande inte är kända i förväg men meddelandet måste ändå behandlas konfidentiellt. Det kan exempelvis röra sig om dokumentation som flera är behöriga att läsa men det går inte i förväg att säga vilka dessa personer är. Ett exempel på detta är patientjournaler, där läkare, sjuksystrar, patienten med flera har rätt att läsa innehållet men inte allmänheten. *Attributbaserad kryptering* (ABE)[8] skapades för att hantera kommunikation med okända mottagare som istället för identifiering uppfyller en policy för att ta del av innehållet. På så sätt kombineras kryptering med åtkomstkontroll.

ABE baseras på asymmetrisk kryptering och har sitt ursprung i identitetsbaserad kryptering[9]. I ABE definieras ett antal attribut och dessa kopplas samman med en policy vilket om alla rätta attribut redovisas beviljar åtkomst till filen, det vill

[8] Eng. Attribute-Based Encryption, ABE.

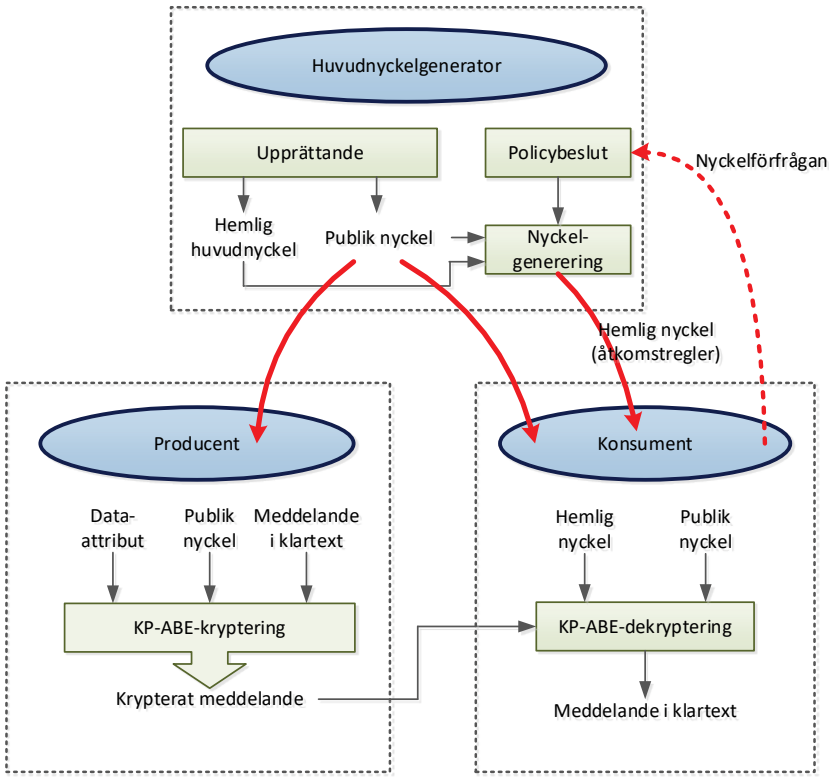
[9] Identity-Based Encryption, IBE.

säga filen dekrypteras. En fil med antingen en uppsättning attribut alternativt en policy kopplad till sig benämns som ett informationsobjekt.

ABE implementeras huvudsakligen i någon av två modeller: *Key-Policy ABE* respektive *Ciphertext-Policy ABE*, vanligtvis förkortat KP-ABE respektive CP-ABE. Gemensamt för båda modellerna är att de behöver använda en huvudnyckelgenerator[10] (MKG) för skapande och hantering av nycklar.

I en KP-ABE-lösning skapas informationsobjektet av en producent genom att en uppsättning attribut knyts till den nyckel som krypterar den fil som informationsobjektet innehåller. Den konsument som vill läsa dokumentet behöver en motsvarande nyckel som innehåller en policy för vad innehavaren av nyckeln får ta del av. Då konsumentens nyckel med policy är personlig innebär det att två olika konsumenter kan läsa vissa gemensamma informationsobjekt krypterade med samma nyckel och attribut men inte andra där andra attribut har använts. En överblick av KP-ABE presenteras i Figur 3.

[10] Från eng. Master Key Generator, MKG.



Figur 3 Key-Policy Attribute-Based Encryption, KP-ABE[11]

Huvudnyckelgeneratorn i Figur 3 skapar ett asymmetriskt nyckelpar där huvudnyckelgeneratorns publika nyckel kommer att används som gemensam kunskap för producenten och konsumenten. Producenten av ett informationsobjekt använder huvudnyckelgeneratorns publika nyckel tillsammans med en uppsättning attribut för att skapa ett informationsobjekt. Producenten har nu ett krypterat informationsobjekt som kan distribueras, exempelvis genom att tillgängliggöras via en webbtjänst. Konsumenten laddar ner informationsobjektet och begär huvudnyckelgeneratorns publika nyckel samt en hemlig nyckel som innehåller konsumentens policy. Om konsumentens policy stämmar med attributen i informationsobjektet dekrypteras det. Om producenten fortsätter att kryptera informationsobjekt med samma publika nyckel från huvudnyckelgeneratorn och konsumentens policy inte förändras, behöver inte någon av

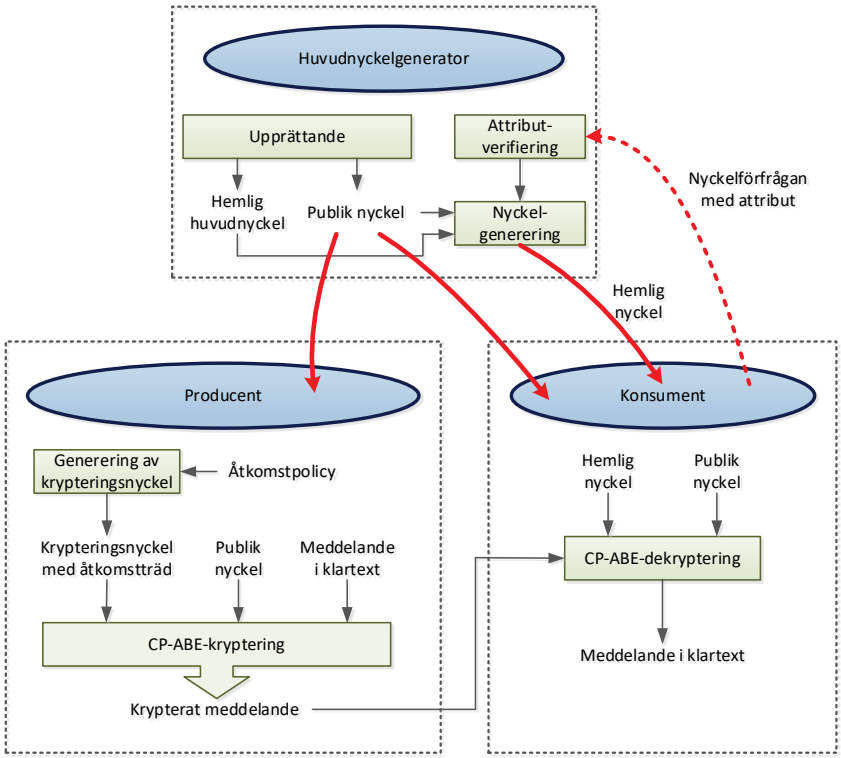
[11] Figur från Westerdahl, Hunstad och Mörnestedt (2014a).

parterna därefter ha kontakt med huvudnyckelgeneratorn, så länge den publika nyckeln är giltig.

CP-ABE vänder på förhållandet attribut och policy. I CP-ABE fästs policyn tillsammans med den fil som utgör innehållet i informationsobjektet och som man vill reglera åtkomst till. Konsumentens dekrypteringsnyckel kommer då att innehålla ett antal attribut som beskriver konsumenten och som policyn får värdera. En överblick av CP-ABE presenteras i Figur 4.

Precis som för KP-ABE skapar huvudnyckelgeneratorn i Figur 4 ett asymmetriskt nyckelpar där den publika nyckeln utgör den gemensamma kunskapen. Producenten hämtar huvudnyckelgeneratorns publika nyckel och krypterar den fil som informationsobjektet ska innehålla med den publika nyckeln samt en policy som producenten skapat. Därefter kan informationsobjektet göras tillgängligt på lämpligt sätt. Konsumenten hämtar hem informationsobjektet och begär den publika nyckeln från huvudnyckelgeneratorn samt sin hemliga nyckel innehållande ett antal beskrivande attribut. Om konsumenten har de attribut som policyn kräver dekrypteras informationsobjektet. I CP-ABE finns således en policy för informationsobjektet medans konsumenter kan ha olika attribut kopplade till sig och sin hemliga nyckel. Så länge en konsument innehar de attribut som krävs för att uppfylla policyn kommer informationsobjektet att dekrypteras, även om två konsumenter kan ha olika attribut i övrigt.

I en jämförelse är KP-ABE mer centraliserad i sin policyhantering i och med att konsumenten tilldelas en policy av huvudnyckelgeneratorn. I CP-ABE har producenten själv möjlighet att bestämma en lämplig policy.



Figur 4 Ciphertext-Policy Attribute-Based Encryption, CP-ABE[12]

Till skillnad från ABAC som har tillämpats i verkliga system, så är ABE än så länge mer forskningsorienterat. Den vanligaste tillämpningsmiljön för ABE är patientjournaler, då sjukhusmiljöns tidigare beskrivna problembild med flera behöriga läsare av en journal är svår att lösa med traditionell kryptering. Det är främst CP-ABE som använts vid tillämpningar men det finns även exempel för KP-ABE där olika policyer behöver tillämpas på en källa (informationsobjekt). Ett exempel som nämnts är olika behörigheter att ta del av en strömmande tjänst. Producenten, till exempel en kabel-TV-leverantör, distribuerar allt sitt material över en kanal men vad konsumenten kan se beror på dennes abonnemang, det vill säga vilken policy konsumenten har (Goyal, Pandey, Sahaiz & Waters 2006).

[12] Figur från Westerdahl, Hunstad och Mörnestedt (2014a).

Genom att åtkomstbeslutet först beviljas när ett informationsobjekt ska dekrypteras hos en konsument, sker detta lokalt. Detta innebär, när alla nycklar är distribuerade, att en konsument kan få tillgång till ett informationsobjekt utan att behöva hämta informationsobjektet från producenten. Det kan distribueras via en webbtjänst eller offline, exempelvis via ett portabelt minne, med bevarad åtkomstpolicy. Vidare adresserar ABE grupper av användare, snarare än individer. Det gör att det går att skapa informationsobjekt som kan fortsätta att användas i framtiden utan att kommande läsare är kända i förväg. En uppenbar nackdel med att en policy är länkad till ett informationsobjekt är att policyn då kommer att gälla så länge filen finns och har en giltig nyckel. Det innebär att om en policy ändras (i fallet med CP-ABE) måste informationsobjektet krypteras om. Det gamla informationsobjektet finns dock kvar om den distribuerats och kommer även den vara giltig så länge som giltighetstiden för huvudnyckel-generatorns publika nyckel är satt.

Med ABE följer även ett annat tankesätt kring säkerhet och åtkomst. Säkerhet beskrivs traditionellt med triaden konfidentialitet, riktighet och tillgänglighet, där konfidentialitet skyddar informationen, riktighet ser till att den är oförändrad och tillgänglighet att den kommer en behörig användare till handa i tid. För ABE, framför allt om den tillämpas i en molnmiljö, ligger fokus på konfidentialitet och riktighet. Ansvaret för tillgängligheten flyttas till den som distribuerar informationen, exempelvis en molnleverantör (Kiviharju 2017).

3.3 Annan forskning och initiativ

Säker informationsdelning är en utmaning för alla länders försvarsmakter. Särskilt i koalitioner har detta uppmärksammats, då behovet av snabb informationsöverföring mellan samverkande system blir tydligt. På en övergripande nivå finns arbetet inom *Federated Mission Networking* (FMN) vilket är ett system för att skapa en gemensam informationsdomän. I arbetet deltar Nato tillsammans med 34 enskilda nationer. Målet med FMN är att skapa ett informationsdelningssystem som kan bli operativt så fort ett beslut om samarbete fattas. Denna ambition, på engelska kallad *Zero-day capability*, är kritisk i en koalitionsmiljö där koalitionspartners tillkommer och lämnar koalitionen när deltagande styrkor roterar eller nationella politiska beslut medför förändringar. De utvecklingssteg som tas inom FMN-arbetet syftar till en gradvis utveckling av förmågan till att dela information på ett säkert sätt. Behovet av en hög grad av automation rörande konfidentialitet vid informationsdelning identifierades tidigt, då dåvarande lösningar var manuella. Kraven på förmågan att dela information har sedan länge passerat vad en manuell hantering kan klara av.

Förmågan att säkert kunna dela information med andra nationer var tidigare mest prioriterat i koalitionssammanhang. Numera är det dock ett nationellt behov för Sverige genom bilaterala avtal och det värdlandsavtal (Neander 2018) som undertecknats. Det finns även ett doktrinärt stöd i *Militärstrategisk doktrin för Sveriges militära försvar* (Försvarsmakten 2016) om förmågan att kunna samarbeta.

En hel del av FMN-forskningen och -utvecklingen har tidigare genomförts inom Natos forskningsprogram, *Science and Technology Organization* (STO). Inom STO finns flera forskningsuppdrag vilka tagit fram delresultat som kan kopplas till dagens FMN-utveckling. *NATO Communications and Information Agency* (NCI Agency) är en Natogemensam fast bemannad forskningsorganisation där forskning kring bland annat FMN har bedrivits. Inom NCI Agency har en lösning för informationsdelning och -hantering tagits fram för exempelvis FMN, kallad *Content-based Protection and Release* (CPR) (NATO Communications and Information Agency 2013). Lösningen är baserad på attributbaserad åtkomstkontroll där attribut om användare, lokala förutsättningar och information om efterfrågad resurs värderas mot en central policy. CPR har dock, till skillnad från en generisk implementation av attributbaserad åtkomstkontroll, två processer implementerade, en för hur information delas (content release) och en för hur information hanteras (content protection). Det innebär att det, förutom krav på kontextvariabler såsom tid och användaren, även ställs krav på den terminal som användaren vill se informationen på. CPR:en är tänkt att implementeras i en *Information Exchange Gateways* (IEG), det vill säga den gränsfunktion som finns mellan två säkerhetsdomäner.

Oudkerk och Wrona (2013) beskriver i ett konferensbidrag på översiktlig nivå hur attributbaserad kryptering kan kopplas till CPR. Bidraget tar upp hur informationsdelningen kan hanteras med stöd av attributbaserad kryptering och hur information därefter kan göras tillgängligt via ett privat Natomoln. Wrona (2015) bygger vidare på dessa tankar genom att beskriva hur *Object-Level Protection* (OLP) kan användas av IoT[13] i en militär kontext. I bidraget diskuteras möjligheterna att använda OLP i ett IoT-sammanhang, men konkluderar samtidigt att moderna krypteringsmetoder kan vara för krävande för flera IoT-system. Utvecklingen går dock fort framåt så detta kan vara ett övergående problem.

[13] Internet of Things, kallas ibland på svenska för Sakernas internet

Just behovet av beräkningskraft och bandbredd är ett tydligt militärt problem, exempelvis i ad-hoc-nätverk[14]. Särskilt påtagligt blir det i ett sensornätverk där sensorerna kan vara mycket små och inte har möjlighet till någon extern energiförsörjning. Vidare så kan bandbredden i rörliga taktiska nätverk vara begränsad, vilket kan vara hämmande för kommunikationsförmågan. Kiviharju och Kurnikov (2016) tar upp kommunikationskostnader för tillgängliga ABE-implementationer då de, beroende på hur detaljerad policy informationsobjekten bär med sig, skapar ett relativt stort overhead i förhållande till volymen på nyttoinformationen. Författarna rekommenderar att endast använda ABE som en lösning för större dokument och där policyn avser hela dokumentet. Samtidigt anser de att tekniken och dess möjligheter är lovande och värd att vidareutveckla.

Behovet av att kunna värdera egenskaper hos information baserat på andra värden än konfidentialitet har behandlats inom ett STO-forskningsprojekt. Resultatet har publicerats som ett konferensbidrag (Melrose et al. 2016), där värderingsformat för riktighet och tillgänglighet analyseras.

Kanada var tidigt ute med att skapa system för gemensam informationshantering för olika informationssäkerhetsklasser och domäner. *Secure Access Management for Secure Operational Networks* (SAMSON), är ett system som hanterar åtkomstkontroll i en befintlig nätverksstruktur. Det innebär att SAMSON följer principerna från attributbaserad åtkomstkontroll (avsnitt 3.1) med en PEP som fångar upp en begäran om en fil, värderar den utifrån filens och användarens attribut samt rådande policy och, om allt stämmer, dekrypterar och skickar den begärda filen (Simmelink, Charlebois, Carruthers & Henderson 2016). SAMSON:s säkerhetslösning ligger och lyssnar av den normala nätverkstrafiken, vilket medför att inga förändringar behöver göras i befintliga system. Förutsättningarna för att åstadkomma den typ av åtkomstkontroll som SAMSON och attributbaserad åtkomstkontroll kräver, är att informationen är märkbar, oftast med XML-taggar. Det framgår inte specifikt i Simmelink et al. (2016) hur denna märkning går till. Vad som dock framgår är att det finns behov av att studera märkning av snabbare mänsklig kommunikation såsom chatt, medan vanliga dokumentfiler kan hanteras på annat sätt.

Det som hittills beskrivits har i huvudsak varit implementationer av en övergripande säkerhetsfunktion, motsvarande PEP och PDP i attributbaserad åtkomstkontroll. Grundläggande för att dessa funktioner ska fungera är att det

[14] Eng, Mobile Ad-hoc NETwork, MANET.

finns attribut i form av metadata associerad till information, användare och miljöfaktorer, samt att det går att lita på att associationen är korrekt. Jäarvinen et al. (2018) diskuterar i ett konferensbidrag möjligheter och problem med att fästa metadata i direktmeddelanden[15]. Grunden för bidraget är *The Extensible Messaging and Presence Protocol* (XMPP) och dess extension XEP-0258 för säkerhetsmarkering. Deltagarna i nätverk såsom FMN hanterar dock inte alltid samma protokoll eller protokollversion, vilket medför problem. I Jäarvinen et al. (2018) framgår inte helt oväntat att ju fler olika versioner av XMPP det finns ju svårare blir det att kommunicera säkert. Å andra sidan så föreslås även en proxylösning inom varje domän, vilken i bästa fall kan konvertera gamla eller proprietära metoder till en sammanhängande metod för metadata.

[15] Eng. Instant Messaging (IM).

4. Analys

Den grundläggande tanken inom datacentrerad säkerhet (DCS) är att fokus primärt läggs på att värdera innehållet i informationen, inte platsen där informationen lagras. Teknikerna attributbaserad åtkomstkontroll (ABAC) och attributbaserad kryptering (ABE) som presenterades i kapitel 3 är två helt skilda lösningar för att uppnå detta.

I resterande del av detta kapitel kommer ABAC och ABE att analyseras utifrån de principer som identifierats i (PKWARE 2019): *Central säkerhets-förvaltningsfunktion*, *Sömlöst skydd*, *Automatiserade säkerhetsprocesser* samt *Anpassningsförmåga*.

4.1 Attributbaserad åtkomstkontroll

ABAC tillämpas på en klient-serverlösning där förfrågningar om åtkomst till en fil fångas upp och värderas av ett system av uppslagstjänster för policyer och attribut som beskriver konsumenten, filen och miljöattribut. Systemet förutsätter kunskap om vilka användare som finns inom systemet samt en förmåga att ta in vilka förutsättningar som omger konsumenten just nu. Själva åtkomstbeslutet fattas i anslutning till där den efterfrågade filen är sparad. Content Protection and Release (CPR) och *Secure Access Management for Secure Operational Networks* (SAMSON) tillämpar båda ABAC för att uppnå åtkomstkontroll.

4.1.1 Central säkerhetsförvaltningsfunktion

ABAC bygger på att en central policy konsulteras vid varje förfrågan om åtkomst till en fil. Funktionen *Policy Enforcing Point* (PEP) fångar upp alla förfrågningar riktade till den server där aktuell fil är lagrad. Genom att PEP är en tvingande funktion får policyförändringar snabbt genomslag i de system som policyn förvaltar. I och med att åtkomstbeslutet fattas av centrala system finns det stora möjligheter att implementera övervakningsfunktioner vid exempelvis en PEP.

För att ett attributbaserat system ska vara effektivt krävs dels att det finns en uppsättning bestämda attribut att tillgå. Detta för att undvika nyanser av samma attribut, exempelvis felstavningar, men även för att definitionen av attributen måste vara densamma för policyskapare och åtkomstkontrollsystem.

4.1.2 Sömlöst skydd

I och med att ABAC endast hanterar åtkomstkontroll finns det inga definierade skyddsmekanismer för filer då de transporteras eller lagras. Behovet av skydd

vid transport och lagring är dock känt och får hanteras i de system som tillämpar ABAC. Precis som för traditionella åtkomstsystem går det dock inte att säga något om hur filer hanteras efter det att en behörig konsument mottagit dem.

Det finns stora möjligheter för ABAC att agera plattformsoberoende. Tekniken bygger på en tjänstebaserad arkitektur och det finns en standard för att implementera ABAC.

4.1.3 Automatiserade säkerhetsprocesser

Den tjänstebaserade arkitekturen bygger på öppna standarder. ABAC implementeras så att den fångar upp förfrågningar till aktuell server. På så sätt kan åtkomstkontrollen placeras mellan en konsument och en producent utan att stora förändringar behöver göras i befintliga system.

En förutsättning för att säkerhetsfunktionerna ska fungera är att det finns attribut som beskriver filer, konsumenter och miljöfaktorer. Det innebär dels att det behöver finnas en uppsättning fördefinierade attribut enligt avsnitt 4.1.1, dels att dessa måste skapas automatiskt. ABAC innehåller ingen styrning för hur eller vilka attribut som skapas eller när detta sker.

4.1.4 Anpassningsförmåga

Genom att det finns standarder som realiserar ABAC och att dessa standarder är skapade genom internationella sammanslutningar så bör ABAC-lösningar kunna hantera förändringar i den lokala infrastrukturen.

4.2 Attributbaserad kryptering

Attributbaserad kryptering (ABE) är en kryptografiskt baserad lösning där användarattribut och åtkomstpolicy knyts direkt till en fil och en användare. Genom att knyta användarattribut eller åtkomstpolicy till en fil skapas ett informationsobjekt som kan förflyttas fritt utan hänsyn till vem som äger eller ansvarar för den plats där informationsobjektet för tillfället är lagrat. Åtkomstbeslutet i en ABE-lösning fattas lokalt hos konsumenten när denne försöker dekryptera informationsobjektet. Ett informationsobjekt, när det väl är skapat, kan därmed få en högre tillgänglighetsgrad avseende var informationen kan lagras. De tillämpningar av ABE som hittills observerats finns inom forskningsvärlden, främst med inriktning mot patientjournaler.

4.2.1 Central säkerhetsförvaltningsfunktion

Inom ABE har Huvudnyckelgeneratorn (MKG) en central roll. Det är genom den som producenten får tillgång till en nyckel för att kryptera ett informationsobjekt och konsumenten får tillgång till de nycklar som behövs för att dekryptera motsvarande fil. De båda varianterna av ABE, Key-Policy ABE (KP-ABE) och Ciphertext-Policy ABE (CP-ABE), har olika grad av central styrning. KP-ABE är mest centralt kontrollerad i och med att MKG:n genererar den policy som gäller för konsumenten. CP-ABE lämnar över ansvaret för skapande av en policy till producenten genom att förse producenten med en nyckel för att kryptera aktuellt informationsobjekt.

I och med att ABE bygger på krypteringsmekanismer finns inte samma flexibilitet när det gäller förändring av en policy. När en konsument, i fallet KP-ABE, hämtat sina nycklar från en MKG kan denne alltid dekryptera det informationsobjekt som är baserad på en MKG:s publika nyckel så länge konsumentens policy är giltig. I ett CP-ABE-system kan en konsument dekryptera ett informationsobjekt så länge dennes attribut är tillräckliga för att tillfredsställa den policy som är kopplad till aktuell fil. Konsekvensen av detta blir att det är kostsamt att ändra en befintlig policy eller attribut. För varje policy, vare sig den är knuten till ett informationsobjekt eller en konsument, så gäller den till dess att giltigheten för en MKG:s publika nyckel eller attributen upphört.

Styrkan med att åtkomstbeslutet fattas hos konsumenten när denne vill dekryptera ett informationsobjekt är att attribut eller policy följer med informationsobjektet. Genom att åtkomstkontrollen sker lokalt behöver det inte finnas en koppling mot en central server för att få åtkomst till informations-objektet. Detta möjliggör en offline-distribution och åtkomstkontroll av informationsobjekt som inte är möjlig med exempelvis ABAC.

En konsekvens av att ABE bygger på kryptografi är att producenten och konsumenten måste använda samma MKG, då en MKG:s publika nyckel är det som binder samman producent och konsument. Det innebär att en MKG måste exponeras för alla som ska kunna agera som antingen producent eller konsument.

4.2.2 Sömlöst skydd

En kryptografisk lösning har den fördelen att under transport är informations-objektet skyddat, oavsett hur det transporteras. Informationsobjektet är även skyddat när det lagras, förutsatt att ingen dekrypterat informationsobjektet och sparat den inkluderade filen separat.

4.2.3 Automatiserade säkerhetsprocesser

ABE är mest använd inom forskningsverksamhet. Det finns ett antal implementationer och försöksverksamhet men ännu inte en kommersiell lösning. Det är därför svårt att säga något om hur ABE tillämpas i praktiken. Behovsmässigt finns det, likt ABAC, behov av en uppsättning definierade attribut. Det är dessutom lämpligt att så mycket som möjligt av processen för att skapa informationsobjekt automatiseras. Dels för att säkerhetsställa att det sker, dels för att underlätta för producenter av informationsobjekt.

4.2.4 Anpassningsförmåga

Förändringar avseende policy eller beskrivande attribut kräver att nya informationsobjekt skapas. Detta kan vara kostsamt och bitvis även svårt om informationsobjekten är utspridda på externa lagringsplatser. Det gör att det krävs en viss eftertanke över vilka användningsfall där ABE kan vara en lämplig lösning.

En sammanfattning av ABAC och ABE presenteras i Tabell 1.

Tabell 1 Jämförelse mellan ABAC och ABE utifrån DCS-principer

	ABAC	ABE
Central säkerhets-förvaltningsfunktion	• Central policy • Kontrolleras vid varje förfrågan • Möjlighet till loggning • Kräver god tillgång till metadata	• Central eller producentskapad policylösning • Statisk policy när IO[16] har skapats • Loggning är svårt efter att ett IO släppts iväg. • Kräver att konsument och producent använder samma MKG[17]
Sömlöst skydd	• Inget automatiskt skydd efter åtkomst beviljats • Kan implementeras genom standarden XACML	• Kan skicka IO över vilket media som helst • Inget automatiskt skydd efter åtkomst beviljats
Automatiserade säkerhetsprocesser	• Fångar upp förfrågningar • Ingen automatisk metadataskapande	• Inga mogna tillämpningar att jämföra med • Kräver handpåläggning men kan automatiseras • Ingen automatisk metadataskapande
Anpassningsförmåga	• Ligger ovanpå befintligt system	• Är en större omställning från befintliga system.

[16] Informationsobjekt, IO

[17] Huvudnyckelgenerator, eng. Master Key Generator, MKG

5. Diskussion

Datacentrerad säkerhet (DCS) har under senare år diskuterats som ett säkerhetskoncept för att fokusera på *vad* som är i behov av att skyddas, mera än *var* det befinner sig. En nyfikenhet finns huruvida idéer inom DCS-konceptet kan bidra till att nå Försvarsmaktens mål avseende interoperabilitet och säker informationsdelning. Utöver konceptet DCS existerar andra ansatser till forskning och utveckling med liknande målbilder. FOI har i tidigare projektverksamhet studerat det närliggande säkerhetskonceptet objektbaserad säkerhet (OBS).

För att realisera säkerhetskoncept som DCS och OBS behövs underliggande konkreta tekniska lösningar. Redovisningen i avsnitt 2.1 har ett fokus på DCS som koncept, medan analysen i kapitel 4 däremot fokuserar på hur underliggande tekniska lösningar kan realisera potentialen i konceptet, främst attributbaserad åtkomstkontroll respektive attributbaserad kryptering.

5.1 Mognad

Attributbaserad åtkomstkontroll utgår ifrån en individ för att därefter komplettera med andra egenskaper i syfte att skapa en så adekvat åtkomstkontroll som möjligt. Tjänsteorienteringen och användandet av metadata i XML-format gör också att åtkomstkontrollfunktioner kan byggas ovanpå existerande informationssystem. Detta förutsätter dock att det finns metoder och strukturer för hur information om informationsobjekt och användare märks, något som endast kort omnämns i denna rapport.

Attributbaserad kryptering kan ha en högre tillgänglighetsnivå genom att det i grunden är ett krypteringssystem. Den högre tillgängligheten kommer av att platsen där informationsobjektet lagras inte behöver vara inom den egna domänen. Mottagaren av ett informationsobjekt har, om denne är behörig, tillgång till den nyckel som kan dekryptera informationsobjektet. Om policyn överensstämmer med de attribut som presenteras kan mottagaren dekryptera informationsobjektet. Attributbaserad kryptering har dock inte samma möjligheter att hantera olika typer av behörigheter, utan kan bara avgöra om mottagaren får läsa innehållet i informationsobjektet eller inte. Inom attributbaserad åtkomstkontroll kan även andra behörigheter hanteras, såsom skriva och radera. Att attributbaserad kryptering dessutom kan adressera okända mottagare bryter traditionella säkerhetsmodeller, vilket kan försvåra ett införandebeslut. De försök som gjorts med att koppla attributbaserad kryptering till befintliga implementationer, exempelvis Content-based Protection and Release (CPR), har visat att det är teoretiskt möjligt, men att flera frågor kring säkerhet och prestanda återstår. I och med att det även är en ny metod för att hantera

åtkomstkontroll och kryptering krävs större omställningar av befintliga system för att kunna hantera detta. Det finns dock ett tydligt behov för lösningar som attributbaserad kryptering. Den främsta tillämpningen inom akademisk forskning på attributbaserad kryptering är patientjournaler. I fallet med patientjournaler finns det flera roller som är kända, såsom läkare, sjukvårdspersonal, anhöriga och givetvis patienten själv. Det är dock svårt att i förväg veta vilken läkare eller sjuksköterska som behöver läsa journalen, eller ens på vilket sjukhus detta kommer att ske. De olika rollerna kan dessutom ha olika behörighet för vad de får läsa. En patient kan själv bära med sig sin journal krypterad med attributbaserad kryptering, vilket då även blir en fungerande offline-lösning.

En utmaning som kvarstår inom attributbaserad kryptering, men även för attributbaserad åtkomstkontroll om information lagras krypterad, är hur sökning bland informationsobjekten går till. De attribut som beskriver informationsobjektet måste å ena sidan vara så detaljerade att en policy kan användas för att skapa ett adekvat åtkomstbeslut. Å andra sidan får inte metadata avslöja för mycket om informationsobjektets innehåll, då det skulle motverka syftet med att kryptera informationsobjektet från början.

5.2 Relation till centrala DCS-principer

I avsnitt 2.1 sammanfattas DCS med hjälp av fyra centrala principer:

- central säkerhetsförvaltningsfunktion
- sömlöst skydd
- automatiserade säkerhetsprocesser
- anpassningsförmåga.

De tekniska lösningarna attributbaserad åtkomstkontroll respektive attributbaserad kryptering förhåller sig på olika sätt till de fyra centrala DCS-principerna. Det kan därigenom observeras att idéer på DCS-konceptnivå, inte nödvändigtvis manifesterar sig fullt ut i praktiska tekniska lösningar.

Central säkerhetsförvaltningsfunktion existerar för såväl ABAC som ABE, men innebörden av begreppet skiljer sig en del. Exempelvis är policyskapandet för en undervariant av ABE delegerat till producentnivån, men för övriga centralt förvaltad. Åtkomstkontroll gentemot policy varierar mellan ABE:s statiska förhållningssätt till en tydligare dynamisk i fallet ABAC.

DCS-konceptet förutsätter uppföljande förmågor som rapportering och säkerhetsrevision, vilket kräver loggning. Här är skillnaderna fundamentala mellan de tekniska lösningarna. Attributbaserad åtkomstkontroll stödjer och möjliggör systematisk loggning, men detta gäller inte attributbaserad kryptering.

Den mera långtgående datacentreringen hos attributbaserad kryptering medför att när ett informationsobjekt har släppts ut, finns inte längre någon central funktion som kan handha loggning. Detta är en aspekt som behöver vägas in vid teknikval.

Beroendet av tillgång till väl utformade metadata är centralt för att realisera DCS, bland annat avseende den centrala säkerhetsförvaltningsfunktionen. Rutiner och styrning för skapande av metadata är inte definierade varken för teknikerna ABAC eller för ABE. Detta utgör en fundamental begränsning.

Sömlöst skydd existerar för båda lösningar, men realiserad på olika sätt. I konkreta användningsfall kan det tänkas tillkomma mera detaljerade behov och krav.

Automatiserade säkerhetsprocesser finns i någon omfattning för ABAC, men knappast på den ambitionsnivå som DCS-konceptet förutsätter. ABE:s brist på kommersiell lösning gör det svårt att yttra sig om på vilken nivå automatiserade processer förekommer.

För såväl ABAC som ABE är bristen på rutiner och styrning för skapande av metadata tydlig. DCS-konceptet förutsätter höggradig automatisering, även avseende metadata. Detta utgör en fundamental begränsning i vad som i dagsläget låter sig realiseras av DCS-konceptet.

Avseende *anpassningsförmåga* framträder ABAC som den primära kandidaten.

5.3 Tilltro

Tilltro till DCS måste ta utgångspunkt i tekniska lösningar och vad de kan erbjuda, icke minst i termer av mognadsgrad. Utöver detta är det även av vikt att en organisation som väljer att använda DCS har tilltro till att DCS är i överens-stämmelse med styrande dokument, principer och praxis för organisationen. Människor och organisationer upparbetar traditionellt tilltro till individer och organisationer och där denna tilltro succesivt har upparbetats över tid. DCS utmanar denna syn.

Såväl ABAC som ABE är policybaserade system. Traditionella säkerhetssystem baserar sig på uppslag av förbestämda beslut, exempelvis i form av åtkomst-kontrollistor eller uppslagstjänster. Genom att använda policybaserade system automatiseras beslutet och flyttas till en tidpunkt åtkomsten efterfrågas. Detta medför att det måste finnas en tilltro till de attribut som presenteras och den policy som värderar dessa.

Att införa en central säkerhetsförvaltning med automatiserade säkerhets-processer är en utmaning, även för Försvarsmakten. Utmaningen kräver att

säkerhetspotential kontra risker med DCS granskas närmare utgående ifrån välformulerade fallstudier. Samtidigt talar erfarenheterna från FMN-utvecklingen för att detta är nödvändiga steg att ta. DCS erbjuder här – som koncept – en önskvärd smidighet för att uppnå interoperabilitet och säker informationsdelning.

Relationen mellan DCS-konceptets centrala principer och hur de underliggande tekniska lösningarna uppfyller principerna präglas av ett antal begränsningar. Särskilt utgör bristen på rutiner och styrning för skapande av metadata en fundamental begränsning som kräver ytterligare forskning och utveckling för att uppnå en adekvat tilltro.

Referenser

Försvarsmakten (2016). *Militärstrategisk doktrin för Sveriges militära försvar* (FM2016-7616:1, bil. 1).

Gartner (2014). Gartner Says Big Data Needs a Data-Centric Security Focus. *Newsroom*, 4 juni. https://www.gartner.com/en/newsroom/press-releases/2014-06-04-gartner-says-big-data-needs-a-data-centric-security-focus [2019-11-18]

Goyal, V., Pandey, O., Sahaiz, A. & Waters, B. (2006). Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. I *CCS'06, Proceedings of the ACM Conference on Computer and Communications Security 2006*. Alexandria (VA), 30 oktober-3 november 2006, ss. 89-98. https://eprint.iacr.org/2006/309.pdf

Harrison, S. (2012). It's Time to Move From Net-Centric to Data-Centric. *SIGNAL Magazine*, (February). https://www.afcea.org/content/its-time-move-net-centric-data-centric [2019-11-18]

Hunstad, A.G., Gustafsson, T., Karlzén, H., Mörnestedt, F. & Westerdahl, L. (2012). *Objektbaserad säkerhet - Behov och möjligheter* (FOI-R--3484--SE).

Jäarvinen, J., Marttinen, A., Jäarvinen, R., Carlén, P., Luoma, M., Peuhkuri, M. & Manner, J. (2018). Enabling XEP-0258 Security Labels in XMPP. I *Milcom'18, Military Communications for the 21st Century*. Los Angeles (CA), USA 29-31 oktober 2018.

Kiviharju, M. (2017). *Enforcing Role-Based Access Control with Attribute-Based Cryptography in MLS Environments*. 2 uppl., Tampere: Juvenes Print.

Kiviharju, M. & Kurnikov, A. (2016). Tactical CAC Profile for NATO OLP? Performance Estimations for NATO OLP Cryptographic Evolution Stage. I *MILCOM'16, The 35th Military Communications Conference*. Baltimore (MD), USA 1-3 november 2016.

Melrose, J., Wrona, K., Guenther, K., Haakseth, R., Nordbotten, N. & Westerdahl, L. (2016). Labelling for integrity and availability. I *ICMCIS'2016, 2016 International Conference on Military Communications and Information Systems*. Bryssel, Belgien 23-24 maj 2016. DOI: 10.1109/ICMCIS.2016.7496583

NATO Communications and Information Agency (2013). *Content-based Information Protection and Release in NATO Operations*.

Neander, M. (2018). FMN bidrar till att öka interoperabiliteten när det gäller ledningsstödsystemen. *TIFF*, 3, ss. 4-6.

OASIS (2013). *eXtensible Access Control Markup Language (XACML) Version 3.0*. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf

O'Connor, R. (2018). Data-Centric Security: The Changing Landscape. *Experts-Perspectives* [blogg], 18 oktober. https://www.symantec.com/blogs/expert-perspectives/data-centric-security-changing-landscape [2019-11-18]

Oltsik, J. (2015). *Data-centric Security: A New Information Security Perimeter*. Enterprise Strategy Group.

Oudkerk, S. & Wrona, K. (2013). Cryptographic Access Control in support of Object Level Protection. I *MCC'13, 2013 Military Communications and Information Systems Conference*. St.-Malo, Frankrike 7-9 oktober 2013. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6695501

PKWARE (2019). *A Blueprint for Data-Centric Security*. https://pkware.cachefly.net/webdocs/pkware_pdfs/us_pdfs/white_papers/WP_Data_Centric_Security_Blueprint.pdf

SANS (2019). Data-Centric Security. Kursmaterial från *SEC530: Defensible Security Architecture and Engineering*.

Simmelink, D., Charlebois, D., Carruthers, B. & Henderson, G. (2016). *Secure Access Management for Secure Operational Networks (SAMSON) - Project Management Closeout Report* (DRDC-RDDC-2016-D008). Defence Research and Development Canada.

Westerdahl, L., Hunstad, A.G. & Mörnestedt, F. (2014a). *Object-Based Security with Attribute-Based Encryption - A feasibility study* (FOI-R--4002--SE).

Westerdahl, L., Hunstad, A.G. & Mörnestedt, F. (2014b). *Objektbaserad säkerhet – Sammanfattning av projektet* (FOI-R--4011--SE).

Wrona, K. (2015). Securing the Internet of Things a military perspective. I *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. Milan, Italien 14-16 december 2015. DOI: 10.1109/WF-IoT.2015.7389105

FOI

ISSN 1650-1942

www.foi.se