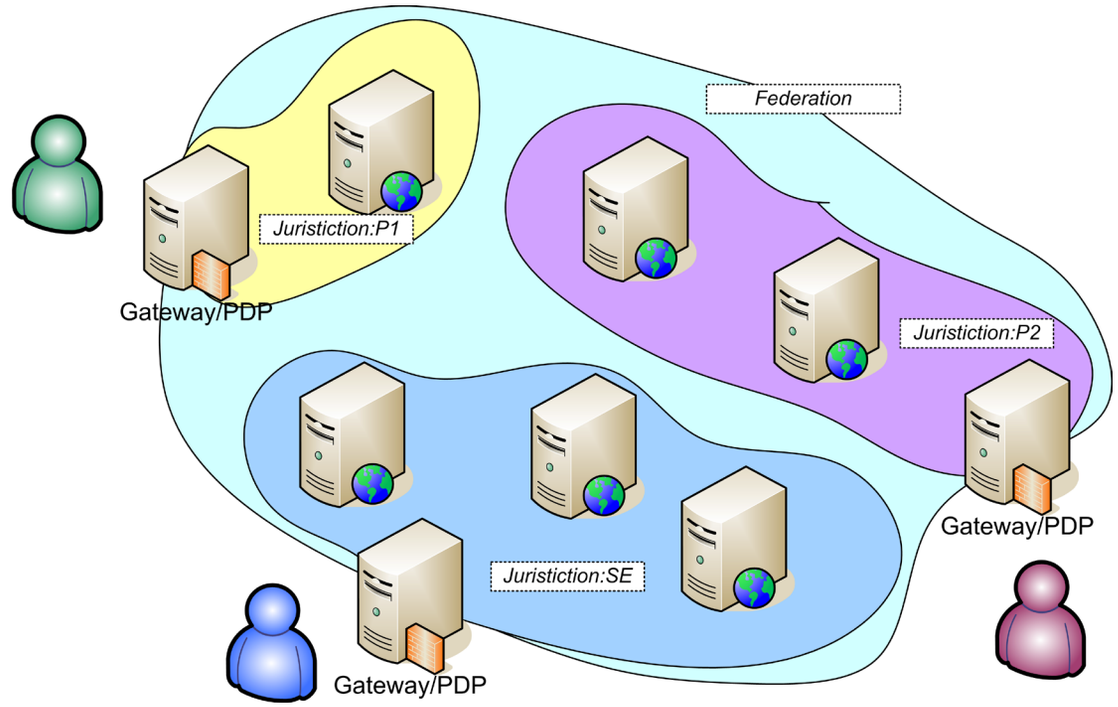
Nättjänster i koalitioner, säkerhetsfrågeställningar

Slutrapport

LARS WESTERDAHL, ALF BENGTSSON



FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
Informationssystem
Box 1165
581 11 Linköping

Tel: 013-37 80 00
Fax: 013-37 81 00

www.foi.se

FOI-R--2668--SE
ISSN 1650-1942

Användarrapport
December 2008

Informationssystem

Lars Westerdahl, Alf Bengtsson

Nättjänster i koalitioner, säkerhetsfrågeställningar

Slutrapport

Titel	Nättjänster i koalitioner, säkerhetsfrågeställningar - Slutrapport
Title	Web-based services in a coalition, security issues – final report
Rapportnr/Report no	FOI-R--2668--SE
Rapporttyp Report Type	Användarrapport User report
Månad/Month	December/December
Utgivningsår/Year	2008
Antal sidor/Pages	34 p
ISSN	ISSN 1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde Programme area	7. Ledning med MSI 7. C4I
Delområde Subcategory	71 Ledning 71 Command, Control, Communications, Computers, Intelligence
Projektnr/Project no	E7153
Godkänd av/Approved by	Pär Carlshamre

FOI, Totalförsvarets Forskningsinstitut
Avdelningen för Informationssystem
Box 1165
581 11 Linköping

FOI, Swedish Defence Research Agency
Information Systems
Box 1165
SE-581 11 Linköping

Sammanfattning

Detta är slutrapporteringen för projektet *Nättjänster i koalitioner, säkerhetsfrågeställningar*. Projektet har studerat möjligheter att med relativt kort förberedelsetid kunna upprätta ett kommunikationssystem med tidigare okända parter. För att dela med sig av information och tjänster antas de blivande medlemmarna vilja ha möjlighet att kontrollera hur deras information och tjänster utnyttjas.

Den lösning som föreslagits är ett webbaserat system som bygger på öppen och tillgänglig programvara, främst Distributed Access Control System (DACS) och rollbaserad accesskontroll (RBAC).

Nyckelord: Rollbaserad accesskontroll, webbapplikationer, webbtjänster, koalitioner, policy decision point

Summary

This is the final report for the project *Web-based services in a coalition, security issues*. The project has studied the possibilities to, on short notice, create a communication system which is to be used with previously unknown partners. In order to be willing to share information and services it is assumed that the participating partners want to be able to control how their information and services are being used.

The proposed solution is a web-based system designed with open source software, mainly Distributed Access Control System (DACS) and role-based access control (RBAC).

Keywords: Role-based access control, web applications, web services, coalitions, policy decision point

Innehållsförteckning

1 Inledning

Under de senaste åren har Försvarsmakten gått från ett invasionsförsvar till ett insatsförsvar. Parallellt har även de internationella uppdragen ökat. Detta ställer andra krav på Försvarsmakten med avseende på samarbetsförmåga. I ett invasionsförsvar var, enkelt uttryckt, Försvarsmakten huvudaktör och andra eventuella aktörer fick anpassa sig. Med ett insatsförsvar är Försvarsmakten, lika enkelt uttryckt som tidigare, en part i ett samarbete för att lösa problem för samhället.

Vilka problem och uppgifter som Försvarsmakten och samhället kan ställas inför är svårt att förutse. En kris kan uppstå hastigt vilken kräver en koordinerad hjälpinsats. Det kan då vara nödvändigt för flera organisationer att, med kort förberedelsetid, samarbeta. Försvarsmakten, civila myndigheter, icke-statliga organisationer och kommersiella företag är alla tänkbara aktörer i ett sådant scenario.

Även om det krävs flera olika aktörer för att lösa en uppgift är det inte nödvändigtvis detsamma som att alla parter är jämställda. Vissa parter kan vara mer betrodda än andra. Detta kan bli särskilt tydligt om det är ett internationellt samarbete där olika nationers försvarsmakter eller organisationer tillfälligt behöver dela information. Här kan det finnas en önskan att reglera tillgången av information och tjänster mellan de olika aktörerna.

Förmågan att samarbeta på en teknisk nivå – att vara interoperabel – är inte bara nödvändig inom Försvarsmaktens olika delar utan även utåt mot det civila samhället och andra försvarsmakter i internationella koalitioner. Det går dock inte i förväg att förutse vilka tekniska system Försvarsmakten skall kunna kommunicera med. Därav finns det en tydlig uttalad styrning att använda kommersiella produkter, vanligtvis benämnda *Commercial Off The Shelf*, eller helt kort *COTS*. Genom att nyttja kommersiella produkter vid systembyggnad ökar sannolikheten att en koalitionspartner skall ha ett liknande, eller i varje fall interoperabelt system.

1.1 Projektbeskrivning

Projektet *Nättjänster i koalitioner, säkerhetsfrågeställningar* har studerat möjligheten att skapa ett system vilket rent tekniskt, baserat på några antaganden, skall vara tillgängligt för vem som helst. Skillnad mellan aktörer görs genom ett behörighetssystem.

1.2 Leveranser

Den huvudsakliga leverabelformen har varit i form av skriftliga rapporter. Totalt har, med denna rapport inräknat, fyra rapporter publicerats av FOI. Två examensarbeten, stödda av projektet, har även publicerats genom Linköpings Tekniska Högskolas försorg.

Ett konferensbidrag [Bengtsson & Westerdahl, 2008] skickades in till *European Conference On Web Services (ECOWS'08)* 2008. Tyvärr antogs inte konferensbidraget till konferensen. Konferensbidraget har kompletterats med implementationserfarenheter och publicerats som ett FOI Memo.

Som avslutning på projektet genomfördes även en demonstrationsdag i Enköping, tillsammans med övriga FoT-projekt inom IT-säkerhetområdet.

En närmare översikt av de levererade rapporterna ges i kapitel 3.3.

1.2.1 Publikationer

Bengtsson, A., Westerdahl, L., *Nättjänster i koalitioner, säkerhetsfrågeställningar – förstudie*, FOI Memo 1752, 2006-05-31

Westerdahl, L., Bengtsson, A., *Publicering i webbapplikationer*, Användarrapport, FOI-R--2142--SE, november 2006

Bengtsson, A., Westerdahl, L., *Access control in a coalition system*, Användarrapport, FOI-R--2393--SE, december 2007

Bengtsson, A., Westerdahl, L., *Access Control in a Web-Based Coalition System, paper with additional comments*, FOI Memo 2558, 2008-10-13

Westerdahl, L., Bengtsson, A., *Nättjänster i koalitioner, säkerhetsfrågeställningar – Slutrapport*, Användarrapport, FOI-R--2668--SE, december 2008

Landberg, F., *Flexible role-handling in command and control systems*, LITH-ISY-EX--06/3855--SE, Linköping, 2006-12-04

Falkcrona, J., *RBAC and SSO for Web services*, LITH-ISY-EX--08/4107--SE, Linköping 2008-03-20

1.2.2 Demonstrationsdag

För att öka förståelsen för de framtagna forskningsresultaten samt för att verifiera möjligheten att tillämpa resultaten genomfördes en demonstrationsdag den 16

september 2008 [Westerdahl, 2008]. Demonstrationsdagen var ett samarbete med de övriga två FoT-projekten inom IT-säkerhet.

Demonstrationsdagen genomfördes med projektvisa demonstrationer på förmiddagen och med en paneldiskussion på eftermiddagen. Paneldebatten leddes av forskningsföreträdaren för FoT Ledning Anders Törne. Panelen bestod av FoT Lednings ordförande Mats Marklund (Försvarsmakten) samt Försvarets materielverks representant Thomas Svensson. Efter paneldebatten fanns utrymme för individuella diskussioner.

1.3 Rapportutformning

Rapporten är utformad enligt följande. Kapitel 2 ger en bakgrund till projektet med en problembeskrivning ur olika synvinklar. I kapitlet presenteras även de tekniker och teknologier som ligger till grund för resultatet. Kapitel 3 beskriver slutresultatet av projektet. Resultatet är uppdelat i tre delar; en teoretisk modell, en demonstrator samt en resumé av tidigare rapporter. I kapitel 4 diskuteras slutresultatet.

2 Bakgrund

I detta kapitel presenteras en problembeskrivning vilken har legat till grund för projektet samt en kortare beskrivning av de metoder som använts. Avslutningsvis ges en beskrivning av de teknologier och tekniker som också utgjort grunden för det erhållna resultatet.

2.1 Problembeskrivning

Problembeskrivningen delas upp i tre aspekter; administrativa, tekniska samt säkerhetsmässiga.

2.1.1 Administrativa aspekter

Insatsförsvaret samt Försvarsmaktens engagemang utomlands ställer högre krav på förmågan att samarbeta med andra organisationer. Dessa organisationer kan vara andra länders försvarsmakter, statliga organisationer, icke-statliga organisationer, kommersiella organisationer (företag), samt icke-kommersiella organisationer. Även inom Försvarsmakten finns behov av samverkan mellan vapengrenarna.

Behovet att samarbeta kan uppstå inom våra egna gränser tillsammans med civila myndigheter likaväl som utomlands med tillgängliga samarbetspartners. I denna rapport definieras samarbetet mellan Försvarsmakten och andra aktörer som en koalition.

I begreppet koalition kan flera tolkningar läggas. Här har koalitioner tentativt definierats som styrkor sammansatta av två eller flera stater med kort förberedelsetid. Det innebär till exempel att det inte förekommit någon längre förberedelsetid för att komma överens om, upprätta och ingå avtal och gemensamma standarder. Lösningarna måste således bli av mer tillfällig art. Likaså har koalitioner ett specifikt syfte och en tidsbegränsad existens. Begreppet kan sättas i relation till benämningen allianser, vilket här anses vara en mer styrd samverkan med ett övergripande syfte snarare än ett specifikt.

Inom både civila och militära system finns det traditionellt en syn vars princip motsvaras av uttrycket ”need to know”. Den som inte har något behov av att veta skall heller inte få tillgång till information. I ett slutet system med fasta strukturer och en någorlunda känd tillämpningsmiljö kan detta fungera för de flesta tänkbara tillämpningar. Svårigheter uppkommer dock när en situation avviker från normen. En sådan speciell situation kan vara en händelse under

vilken en person behöver få tillgång till information denne normalt inte är behörig till.

För att åstadkomma lösningar på nya problem krävs ofta att man samarbetar i andra former än vad som är gängse förekommande. I ett samarbete är det även underförstått att ingående parter behöver dela information med varandra för att en lösning skall uppnås. Således borde ”need to share” vara mer aktuellt än ”need to know”. På en övergripande nivå är det säkert också så, men på en mer konkret nivå är det ofta svårare att dela med sig. Samarbetet försvåras ytterligare om samarbetsparten dessutom är utanför Försvarsmakten.

2.1.2 Tekniska aspekter

Utvecklingen inom informationssystem går allt mer mot att sammankoppla system. Önskan är att en nod skall utföra den deluppgift den är till för och sedan hänvisa vidare till andra noder för att komplettera till dess att hela uppgiften är utförd. Ur en användares perspektiv sker detta mer eller mindre som ett homogent system, även om de ingående systemen kan vara skilda. Generellt går dessa tankar under begreppet *Service Oriented Architecture*, ofta förkortat till SOA. Service oriented architecture är en tjänstebaserad arkitektur där flera tjänster tillsammans levererar en större tjänst. Den vanligaste implementationen av Service Oriented Architecture är *Web Services*, vilket är ett så kallat löst kopplat system. Web Services är mer flexibelt jämfört med tidigare system såsom CORBA.

Web Services har fått mycket uppmärksamhet de senaste åren. Det har, och görs fortfarande, producerats ett flertal protokoll vilka syftar till att kunna beskriva den information som behöver skickas mellan olika delsystem. Protokollen i sig är ofta enbart beskrivande men med intentionen att de skall få ett sådant genomslag att flertalet tillverkare accepterar dem.

För att Web Services skall fungera som det är avsett krävs en stor uppbyggnad av kringliggande system. Först och främst måste ett befintligt system anpassas för Web Services. Därtill måste det skapas ett flertal katalogtjänster för att hantera var de individuella tjänsterna finns och hur de kan göras tillgängliga. För att realisera Web Service fullt ut krävs en omfattande infrastruktur Det har medfört att Web Services inte fått genomslag på nationell eller internationell nivå. Dock finns det flera lösningar där Web Services används i lokala system.

Behovet av Web Services uppkom av att det fanns flera lokala system där systemägarna ville kunna erbjuda sina förmågor i form av tjänster utåt. Befintliga system var dock inte alltid anpassade för att kunna samarbeta med andra system. Ofta handlade det om sökningar i databaser och stordatorsystem eller att

presentera mer eller mindre statisk information. Interoperabilitet var inte ett ledord när dessa system skapades. Att modifiera skulle bli mycket kostsamt, då det i flera fall skulle innebära att ett helt nytt system måste skapas. Med Web Services kunde man skapa ett lager mellan befintliga lokala system via ett mer interaktivt och öppet gränssnitt.

Web Services kan ibland uppfattas som ”pratigt”. Med det avses den stora mängden stödprotokoll som behövs för att skicka ett meddelande samt storleken på dessa. Ett alternativ är Representational State Transfer, vanligtvis förkortat till REST. Med REST går man tillbaka till den mer ursprungliga idén med att alla resurser på nätet skall vara unikt identifierbara och att systemen skall vara löst sammankopplade.

2.1.3 Säkerhetsmässiga aspekter

Säkerhetsmässiga egenskaper beskrivs ofta övergripande i termer av konfidentialitet, integritet och tillgänglighet. Med konfidentialitet avses i första hand sekretess och förmågan att hålla någonting hemligt. Integritet beskriver hur väl ett informationsobjekt är skyddat mot obehörig förändring. Tillgänglighet avser förmågan att tillgodose att informationen görs tillgänglig till dem som har rättighet samtidigt som icke-behörig tillgång skall motverkas.

Konfidentialitet och tillgänglighet kan ofta ses som varandras motsatser. Ser man det mer som en förmåga att kunna ge tillgång till en hemlighet enbart till dem som är behöriga så finns dock ingen direkt motsats. Insamlad information som inte kan nås av behöriga användare är allt som oftast meningslös. För ett system som har som mål att vara snabbt att etablera och ha en hög förmåga att kommunicera med andra system är tillgänglighet viktig. Den information som är tänkt att lagras och transporteras inom koalitionssystemet förutsätts vara icke-hemlig, eller krypterad, vilket i viss mån minskar behovet av sekretess.

Att en viss information inte är hemlig är inte detsamma som att informationen är fritt tillgänglig för alla som skulle vilja ta del av den. Förmågan att styra vem eller vilka som får ta del av informationen är väsentlig. I koalitionssammanhang handlar det även om trovärdighet avseende att kunna hantera informations-säkerhet gentemot de andra koalitionspartnerna. En koalitionspartner kan vilja styra tillgången på den information eller de tjänster som denne tillför beroende på vilka andra som ingår i koalitionen. Det kan till exempel mycket väl vara så att Försvarsmakten under en insats vill dela viss information med myndigheter men inte med privata och icke-statliga organisationer.

Det är svårt att bygga ett generellt system för oförutsedda uppgifter och samtidigt få det effektivt. Ofta är informationssystem uppbyggda efter individer. Det

innebär att rättigheter och styrning av information sker mellan de aktiva individer som ingår i systemet. Vid ett väl uppbyggt system innebär detta oftast inga problem så länge alla nödvändiga individer är aktiva och att förändringar sker kontrollerat. Problem kan dock uppstå om en individ inte är anträffbar eller försvinner ur systemet. Då kan meddelandekedjan eller delegeringssystem mycket väl brytas med den följden att information kan försvinna eller hamna i en ”återvändsgränd”, det vill säga hos en instans som inte vet hur meddelandet skall behandlas. Någon form av inbyggd struktur till exempel rolldefinitioner är lämplig för att skapa kontinuitet i ett system. Med kontinuitet är det möjligt att upprätthålla grundläggande säkerhetsegenskaper. Denna struktur bör kunna bevaras även om användare registreras eller tas bort från systemet.

2.1.4 Sammanfattning

Sammanfattas de administrativa, tekniska och säkerhetsmässiga aspekterna framkommer behov av ett system vilket skall vara så pass generellt att det är interoperabelt med flertalet ospecificerade men generella system. Vidare behövs en mekanism för att kontrollera tillgången till den information och de tjänster som systemet omfattar. Till sist finns det även ett behov av att systemet skall innehålla någon form av grundstruktur för att säkerställa kontinuitet.

2.2 Metod och avgränsningar

Projektet har utnyttjat olika metoder för datainsamling.

2.2.1 Metod

Projektet har i huvudsak bedrivits som en litteraturstudie. Inledningsvis genomfördes en riktad enkätundersökning. Urvalsgruppen var personer på nyckelpositioner inom ledningssystemutveckling inom Försvarsmakten och Försvarets materielverk. Syftet var att fastställa Försvarsmaktens inställning till hur koalitioner skapas och vilka systemegenskaper som är prioriterade i en sådan situation. Resultatet från enkäten låg sedan till grund för den fortsatta litteraturstudien.

Parallellt har även en demonstrator framtagits i syfte att praktiskt påvisa de teoretiska resultaten. Demonstratorn skapades som en del av ett examensarbete men har utvecklats efterhand som projektet fortgått.

2.2.2 Avgränsningar

Det finns en tydlig styrning inom Försvarsmakten att kommersiella produkter (COTS) skall användas i största möjliga utsträckning.

2.3 Ingående teknikområden

Nedan följer en kort beskrivning av de teknologier och tekniker som har legat till grund under framtagandet av resultatet.

2.3.1 REST och Web Services

Inom området tjänster tillgängliga via Internet (Web Services) finns det två dominerande filosofier. Den ena är Simple Object Access Protocol (SOAP) vilket är den mest omtalade, och den andra är Representational State Transfer (REST).

När man talar om Web Services avses oftast XML-formaterade meddelanden paketerade i ett SOAP-meddelande. Ett SOAP-meddelande är likt många andra meddelanden uppbyggt med ett huvud (SOAP-header) och en kropp (SOAP-body). Själva informationen i meddelandet ligger i kroppen. I huvudet finns till exempel metadata och eventuella signaturer till element i kroppen. Tanken med SOAP är att ett SOAP-meddelande skall kunna sändas via vilket nätverksprotokoll som helst. I praktiken har det dock blivit HTTP som är det bärande protokollet och där metoden `POST` används. På nätverksnivå ser alla SOAP-meddelanden likadana ut vilket innebär att standardmässiga metoder för caching och brandväggar inte är tillämpbara. För att dessa metoder skall fungera måste en ”SOAP-cache” eller en ”SOAP-brandvägg” packa upp hela SOAP-medelandet och tolka det, vilket inte är praktiskt tillämpbart. Det är fullt möjligt att skapa flexibla protokoll för att exempelvis hantera säkerhetsfrågor, men det innebär att alla inblandade tjänster måste kunna följa dessa protokoll. En sådan flexibilitet leder ofta till en komplex lösning.

REST använder endast HTTP-kommunikation mellan tjänster. Krav på tillståndslöshet är mycket viktigt för REST-implementationer. Alla metoder som finns i standard HTTP (`GET`, `PUT`, `POST`, etcetera) är tillämpbara. Det innebär också att de vanliga metoderna för caching och brandväggar kan fungera som vanligt.

SOAP kan även beskrivas som ett ”uppifrån och ner”-synsätt där ordning och struktur implementeras och de anslutande enheterna, såsom tjänster och användare, får anpassa sig efter valda regler och protokoll. REST har i det här

resonemanget ett ”nerifrån och upp”-synsätt genom att utnyttja väl etablerade protokoll och deras metoder att hämta information.

En SOAP-arkitektur kan mycket väl vara lämplig när samverkande webbtjänster skall nyutvecklas. I de fall då information skall delas och denna information är nåbar via URL:er är REST ett kanske mer självklart val.

2.3.2 Säkerhetsaspekter i webbaserade system

Webbaserade system har utvecklats i sin förmåga att interagera med nyttjaren. Från att ursprungligen mest ha kunnat presentera statisk information är det numera möjligt att skapa ett mer dynamiskt system. Genom att dela upp systemet i olika lager – presentationslager, logiskt lager samt datalager – skapas en dynamik vilket möjliggör en mer anpassningsbar presentation. En applikation som är uppbyggd på det här sättet brukar kallas för webbapplikation.

En webbapplikation är ett program som presenteras genom en webbläsare. Genom användandet av script och inbäddad kod skapas rika internetapplikationer (eng. Rich Internet Applications (RIA)) [O’Reilly, 2005] vilka ger känslan av att vara lokalt installerade program. Samtidigt har leverantören full kontroll över de data användaren efterfrågar. Både data- och logiklagret finns fysiskt på leverantörens sida, viket ger leverantören full kontroll över dessa. Resultatet blir ett system där leverantören endast behöver underhålla ett centralt system och förändringar får snabbt genomslag hos användarna. En nackdel är det totala beroendet av att vara uppkopplad mot systemet.

Det har skrivits mycket om risker med script i webbläsare och vilka tänkbara hot dessa kan utgöra. Hotbilden har inte på något sätt förminskats med webbapplikationer. Den har snarare ökat. En ökad funktionalitet och interaktion ger en angripare större möjligheter att vara framgångsrik med en attack. Ofta sägs det att ”attackytan” har ökat [Hoffman, 2006].

På senare år har webbaserade attacker som Cross Site Scripting (XSS) och i viss mån även en variant Cross Site Request Forgery (CSRF) fått uppmärksamhet [Higgins, 2006]. Den huvudsakliga orsaken bakom lyckade Cross Site Scripting-attacker är att ovaliderade data tillåts att matas in samt återföras till användaren. Detta öppnar upp för scriptattacker. Cross Site Rrequest Forgery-attacker utnyttjar webbtjänster med svag autentisering där en användare tillåts vara inloggad en längre tid utan att vara aktiv

Syftet med en Cross Site Script-attack är att ta över en session från en användare. Ett sätt att göra detta är att ta kontroll över den cookie som webbapplikationen ofta använder sig av för att hålla lagra det tillstånd användare befinner sig i.

Skarp kritik har riktats mot cookies över åren. Det huvudsakliga problemet med cookies är att en cookie är ett statiskt dataobjekt som kan stjälas. Antag att en användare har en krypterad cookie lagrad på sin hårddisk. Cookien, som innehåller inloggningsstatus för användaren, är då inte läsbar av någon utöver den leverantör som har skapat cookien. Om en angripare lyckas komma över denna cookie behöver denne inte kunna läsa innehållet. Det är fullt tillräckligt att besitta cookien för att en leverantör skall acceptera den. Det innebär att en cookie är ett attribut som användaren vill skydda. Samtidigt är det ett attribut som behöver vara tillgängligt för den domän (leverantör) som skapade cookien.

2.3.3 Accesskontroll

För många system är det inte enbart tillräckligt att veta vem som har rätt till att använda ett system. Det är ofta också nödvändigt att kunna kontrollera vad en användare får göra. Med ett accesskontrollsystem kan systemägaren styra vem som får tillgång till vilka resurser.

Ett accesskontrollsystem består av subjekt (subject), objekt (object), rättigheter (rights) och tillstånd (permission). Ett subjekt behöver inte nödvändigtvis vara en mänsklig användare utan kan mycket väl vara ett annat program. Ett objekt kan till exempel vara en fil, en post i en databas, ett program, eller något annat som är tillgängligt i systemet. Subjektet innehar rättigheter att utföra operationer på ett objekt. Ett objekt ger tillstånd till att vissa operationer får utföras av ett subjekt.

Hur rättigheter är satta beror på vilken säkerhetsmodell som används. En systemägare kan besluta hur all information skall få göras tillgänglig och till vilka. Den modellen brukar beskrivas om *Mandatory Access Control* (MAC). I ett MAC-system styr systemägaren över alla objekt. En användare kan skapa objekt men får inte automatiskt äganderätt eller möjlighet att ändra dem. Ett alternativ till MAC är *Discretionary Access Control* (DAC). Med en DAC-modell är det den som skapat ett objekt som anger vilka andra subjekt som har tillstånd att använda objektet.

2.3.4 Rollbaserad Accesskontroll

I ett större system har ett subjekt flera uppgifter och behov att utföra i systemet. Dessa uppgifter och behov kan variera över tiden. Ur en systemadministratörs perspektiv kan det vara svårt att hålla reda på vilka rättigheter ett subjekt skall ha. Det finns en överhängande risk att ett subjekt inte utrustas med de rättigheter som denne skall ha. Alternativt kan subjektet få för många rättigheter efter hand som det byter uppgifter inom organisationen, vanligtvis kallat rättighetsstegring.

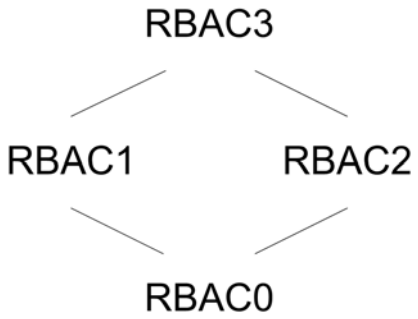
Ett sätt att underlätta hur rättigheter hanteras i ett system är att tilldela dem rollmässigt. De uppgifter ett subjekt utför i ett system beror på vilken position subjektet har i organisationen. Om ett subjekt inte är en människa utan till exempel ett program kan detta program ha beroenden till andra program i någon form av hierarki. Genom att se subjekten efter vilken roll de har i organisationen eller systemet är det enklare att knyta nödvändiga accessrättigheter till den rollen.

En säkerhetspolicy är ofta skriven utefter roller i en organisation. Detta då det oftast är opraktiskt att skriva en policy baserad på individer. Steget till att ha ett system med rollbaserad accesskontroll är då inte långt borta. Det är dock inte uppenbart vad en roll innebär. Definitioner varierar beroende på de syften och behov som finns. Det är enkelt att tänka sig en roll som en grupp användare. I det enklaste fallet kan detta mycket väl fungera men det är inte en korrekt beskrivning.

En roll är en samling tillstånd och subjekt tilldelas roller. En roll beskrivs genom sina rättigheter medan en grupp beskrivs genom sina deltagare. Till exempel kan en användare (subjekt) ha rätt att attestera inköpsordrar, och tillhör gruppen ”attestberättigade”. Men när användaren agerar i rollen ”attestant” kan rollen vara kopplad till regeln ”ej tillåtet att attestera egna ordrar”. En grupp är något man tillhör oavsett vilka uppgifter man utför, medan en roll är något man agerar inom för att utföra en given uppgift.

Ett rollbaserat system är definierat efter Role-Based Access Control (RBAC) referensmodell [Sandhu et al., 1996], avbildad i Figur 1. På den enklaste nivån (RBAC0) omfattar modellen användare (users), roller (roles), rättigheter (rights) och sessioner (sessions). En användare skapar en session och kan inom sessionen använda de roller som denne har tilldelats. Varje roll har en uppsättning rättigheter knutna till sig.

Ibland följer nivån på rättigheterna med i organisationshierarkin. Det är därför



Figur 1: Referensmodell för rollbaserad accesskontroll.

möjligt att skapa en hierarki mellan roller (RBAC1). Med en hierarki är det möjligt att ärva rättigheter mellan olika roller. Ofta finns det även ett behov av att hindra användare från att agera i flera roller samtidigt (RBAC2). I värsta fall kan detta leda till en rättighetsstegring vilken får till följd att en person kan t.ex. både beställa och attestera tjänster i systemet. Genom att införa begränsningar (constraints) på en roll kan man styra så att en användare inte kan vara aktiv i två givna roller samtidigt En konsoliderad modell (RBAC3) uppfyller alla de egenskaper som beskrivits här.

2.3.5 Distributed Access Control System

Distributed Access Control System (DACS) är ett kanadensiskt projekt för reglerad informationsdelning [DACS]. Systemet är uppbyggt i två delar. Del 1 är en samling integrerade funktioner vilka tillsammans erbjuder Single Sign-On, det vill säga att en användare loggar in vid ett tillfälle och att sedan inloggningen följer med även när användaren byter applikation. För en applikation skyddad av DACS innebär det att en användare som vill komma åt applikationen först måste autentisera sig och, om funktionen finns, välja en roll. DACS svarar med att skicka användaren en credential, vilket är en form av värdebevis där DACS intygar att användaren är den som påstås. En credential kan till exempel vara en cookie vilken lagras av användarens webbläsare.

Del 2 ansvarar för att validera accesskontrollfrågor. Alla typer av resurser som kan efterfrågas via URL-anrop (data, exekverbara, scripts, med mera) är associerade till en XML-fil vilken innehåller de accessregler som är uppsatta. DACS tar reglerna från XML-filen, tillsammans med den autentiserade cookien, miljövariabler samt revokeringar. Resultatet blir ett beslut om att godkänna eller avvisa användaren. Det är möjligt att lägga på restriktioner på varje regel. På varje resurs kan det läggas ytterligare restriktioner. De kan då uttryckas som, allow if constraint eller deny if not other constraint. Figur 2 visar en översiktlig bild av DACS.

Den av DACS producerade credential för Single Sign-On följer inte standarden SAML [OASIS (a)]. DACS credential innehåller attribut från DACS egna hierarkiska federationsstruktur. Del 1 har flera likheter med GridShib [GridShib].

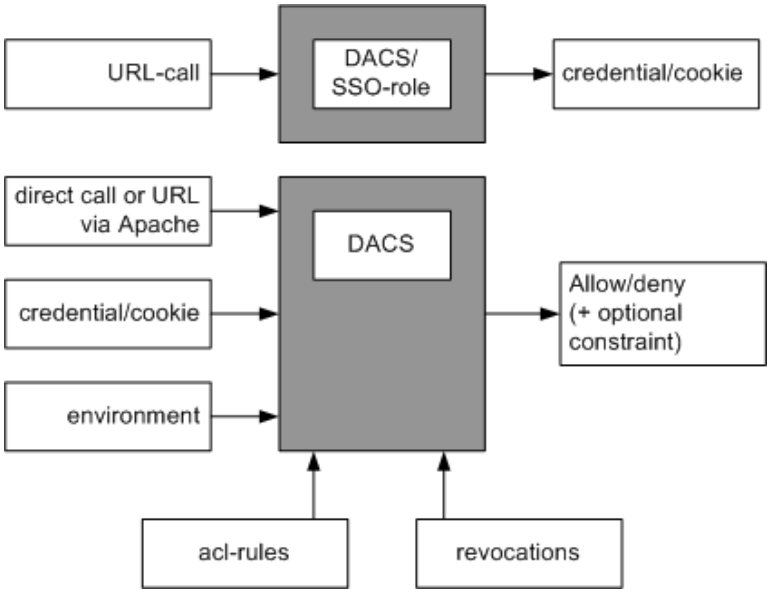
Delen för accesskontroll, del 2, är analog med GRIDs [Globus] accesskontroll. De regler som styr accesskontrollen finns lagrade i XML-element. Det finns stora likheter med standarden XACML [OASIS (b)] men reglerna är inte kompatibla. Accesskontrollen anropas via en utökad modul i Apache. Den credential som skapats i del 1 av DACS följer med anropet. Alla resurser som kan beskrivas med en URL kan kontrolleras. Det omfattar allt från statiska webbsidor till webbapplikationer.

DACS kan konfigureras i en eller flera federationer. En federation är den högsta nivån av identiteter. Inom en federation kan det sedan finnas en eller flera jurisdiktioner (jurisdiction). Inom en federation delar alla en gemensam nyckel vilken används för kryptering och dekryptering av credentials. DACS kan beskriva sina användare hierarkiskt genom dess tillhörighet i en federation och jurisdiktion;

`ID=federation-name:jurusdiction-name:user-name.`

Alla konfigurationer styrs genom XML-formaterade konfigureringsfiler.

Inom en jurisdiktion hanteras användare, grupper och regler. Den lägsta identitetsnivån inom DACS är användarnamn (username). En användare är unik inom den jurisdiktion den tillhör. Ett användarnamn behöver inte vara ett namn



Figur 2: Översikt av DACS.

på en individ, det kan också vara en grupp eller en roll.

DACS har flera fördelar. Främst är det en öppen programvara. Det är också enkelt och flexibelt med flera komponenter testade och integrerade. Till de negativa egenskaperna hör bland annat att DACS än så länge endast finns tillgänglig för UNIX. DACS följer inte heller de standarder som skapats inom OASIS såsom SAML och XACML. Anropen till DACS sker via URL, DACS följer således REST-standarden.

3 Resultat

Inom projektet har en teoretisk modell för informationsdelning genom en webbtjänst framtagits. Som ett ”Proof of Concept” har även en demonstrator utvecklats, vilken visar en avgränsad del av den teoretiska modellen.

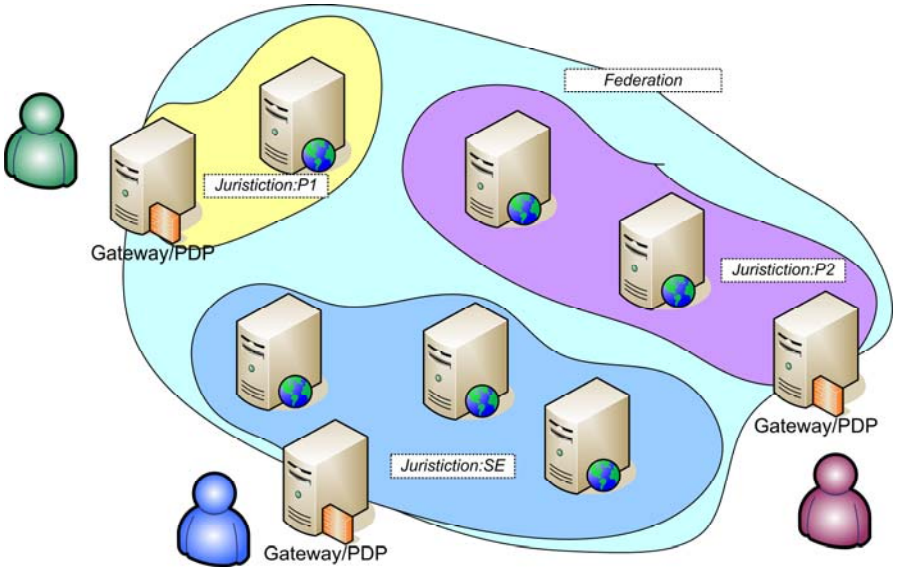
3.1 Koalitionsmodell

I projektets inledning skapades en teoretisk modell över hur en koalition kan vara uppbyggd. En koalition som är skapad under relativt snabba tidsförhållanden har ingen förutbestämd fast struktur. Det gör att modellen måste vara mycket skalbar och flexibel.

Den mest grundläggande tanken med koalitionsmodellen är att alla deltagare i koalitionen vill dela information, samt administrerar egna användare och egen information. En koalitionspartner kan ansluta eller lämna koalitionen under dess existens, likaväl som när den skapas eller upplöses.

I målsättningarna för projektet angavs det att en koalitionspartner själv skall kunna sätta förutsättningarna för nyttjandet av de tjänster som partnern bidrar med. Det innebär att koalitionspartnern själv sätter de rättigheter nyttjarna av tjänsterna tillåts ha.

Figur 3 visar hur koalitionen är uppbyggd. Ett helikopterperspektiv av koalitionen ger att koalitionen är uppbyggd med en yttre gräns kallad federation. Alla inom federationen tillhör koalitionen. De ingående nationerna utgör delmängder av helheten. Varje delmängd utgör jurisdiktion vilken kan omfatta en nation, organisation eller företag. Dessa ansvarar själva för kontroll av de användare som tillhör den egna organisationen.



Figur 3 Översikt av koalitionsidén.

3.1.1 Rättigheter

Tjänster delas inom koalitionen/federationen efter tjänsteägarens gottfinnande . En användare från en jurisdiktion måste således kunna begära och erhålla information och resultat från en annan jurisdiktion. Därav måste det finnas en öppenhet mellan jurisdiktionerna.

En användare autentiserar sig gentemot sin egen organisations autentiserings-system, alternativt mot ett koalitionsgemensamt autentiseringssystem. Användaren kan sedan begära tjänster eller information ifrån de andra organisationerna som ingår i koalitionen. Jurisdiktionerna i sig skall inte utgöra något hinder för informationsutbytet utan mer fungera som administrativa öar för en organisations publicerade resurser.

Varje organisation sätter de rättigheter som följer deras egen säkerhetspolicy för publicerad information eller tjänster. Det gör att olika koalitionsmedlemmar kan få olika tillgång till en viss information eller tjänst beroende på relationen till informations- eller systemägaren. Det kan uppstå fall där vissa koalitionsmedlemmar får tillgång till en viss information eller tjänst medan andra lämnas helt utanför.

3.1.2 Rollhantering

En förutsättning för att flera organisationer skall kunna samarbeta utan större förberedelsetid är att standardmässiga protokoll och produkter används. En annan aspekt av generalisering är att synkronisera hur användare hanteras i ett system. Det är mycket arbete att omdefiniera rättigheter allt efter som användare ansluter eller försvinner.

Ett enklare sätt att hantera användare är att definiera ett antal roller som agerar inom koalitionen. Rollerna är konstanta i det avseende att de inte är organisationsberoende eller ens bemanningsberoende. En roll, till exempel operatör, anger ett antal rättigheter gentemot en tjänst. Operatörsrollen är bestående oavsett om en organisation tillkommer eller lämnar koalitionen.

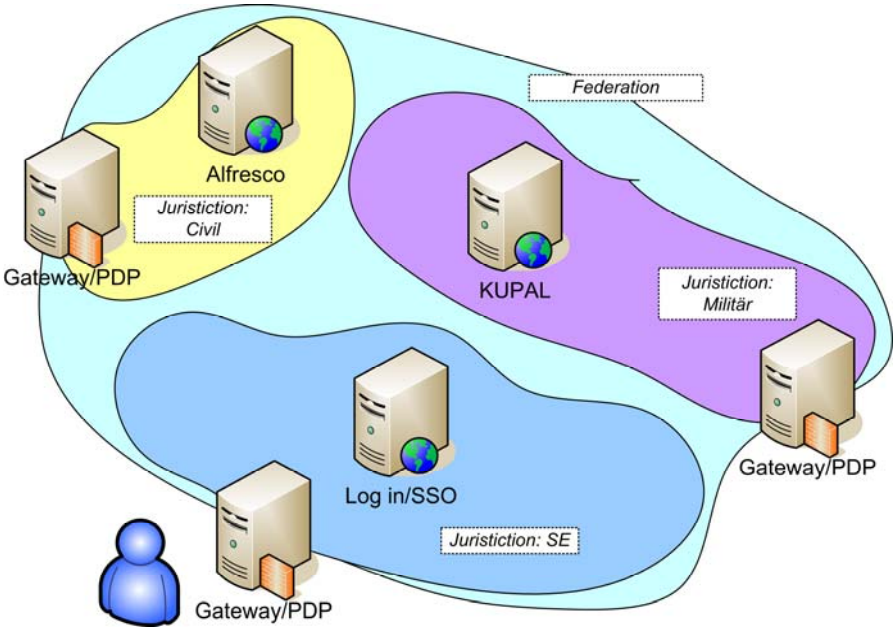
3.1.3 Att lämna koalitionen

Om en organisation väljer att lämna koalitionen är detta ingen komplicerad manöver. Vid inträde och publicering av information och tjänster har ingen kontroll lämnats över till koalitionen. Det innebär att organisationen hela tiden har ansvarat för sin egen utrustning och spridning av information.

3.2 Demonstrator

För att enkelt kunna demonstrera projektets resultat har en demonstrator tagits fram. Demonstratorn är en förenkling av den teoretiska modellen och bygger i grunden på applikationen DACS.

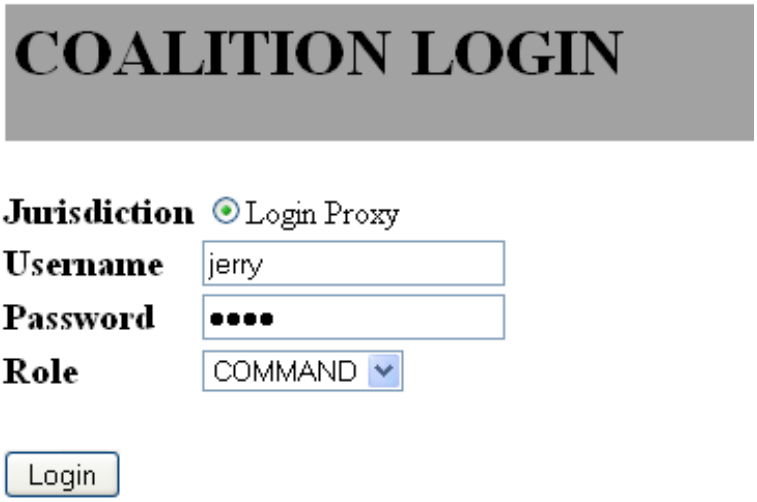
I demonstratorn är endast en applikation per jurisdiktion implementerad inom federationen, se Figur 4. Det görs ingen nations- eller organisationsskillnad på användare i demonstratorn. Användarna autentiserar sig mot ett koalitionsgemensamt autentiseringssystem för Single Sign-On.



Figur 4: Demonstratorarkitektur.

Demonstratorn är implementerad och används ur en jurisdiktions perspektiv, i det här fallet SE, vilket skulle kunna motsvara Sverige. De andra två jurisdiktionerna har här getts tillhörigheten Civil och Militär. SE innehåller en inloggnings- och Single Sign-On-server, samt några enklare webbsidor. Applikationerna som ligger i den civila och militära jurisdiktionen är båda dokumenthanteringssystem (Document Management System (DMS)).

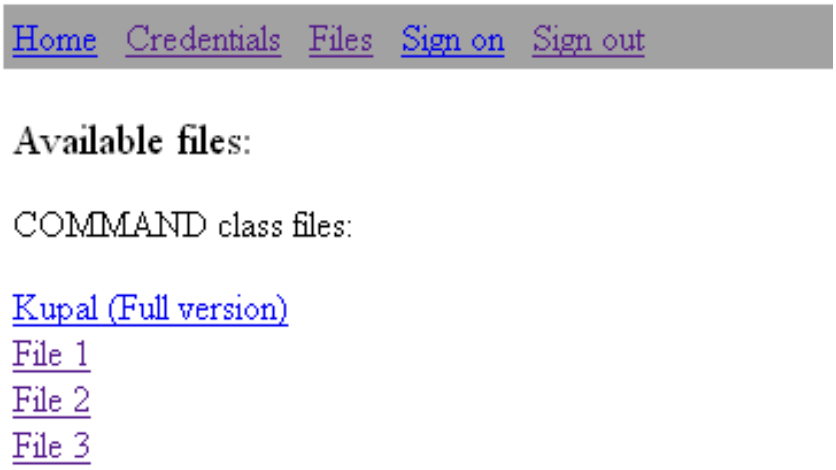
En användare loggar in hos koalitionen genom att autentisera sig hos jursdiktion SE. I samband med autentiseringen väljer även användaren den eller de roller som denne vill arbeta inom. Figur 5 visar inloggningsfönstret.



Figur 5:Inloggning i SE.

DACS stödjer en enklare rollhantering. Den rollhantering som finns i demonstratorn är dock utbyggd för att bland annat klara av att hindra vissa förutbestämda rollkombinationer. En användare agerar inom en viss roll. Vilken rollen är beror på uppgiften. Det betyder också att en användare kan ha flera roller, ibland samtidigt. För att förhindra rättighetsstegring har spärrar implementerats i syfte att hindra en användare att kunna skapa sig för mycket rättigheter i systemet.

En autentiserad användare presenteras ett standardiserat gränssnitt (Figur 6). Vilka länkar och dokument som är tillgängliga varierar med den roll användaren valde.



Figur 6: Dokument och tjänster i demonstratorn.

3.2.1 Tjänster i demonstratorn

Två webbapplikationer har kopplats till auktorisationssystemet; Alfresco i den civila jurisdiktionen samt KUPAL i den militära. Alfresco är en javabaserad dokumenthanteringstjänst vilken är installerad på en Tomcat-server. Tomcat och Apache har en tät koppling viket underlättar kommunikationen mellan Policy Decision Point (PDP) och Alfresco. Den andra tjänsten är KUPAL, vilket är en kunskapsportal för Försvarsmakten och stödmyndigheter till Försvarsmakten. I demonstratorn är en fristående version av KUPAL installerad på en Microsoft ISS-server på en separat dator.

En av de egenskaper som önskas uppnå med rollhantering inom koalitionen är Single Sign-On. Det är rollen som användaren agerar inom som skall vara styrande för vad som får och kan göras med tillgängliga tjänster och informationer. I demonstratorn behöver inte en användare, med en roll som är behörig att använda Alfresco, logga in till applikationen Alfresco, alltså Single Sign-On. Däremot är användaren tvungen att logga in på nytt, till KUPAL, när tjänsten KUPAL önskas.

3.3 Resumé av delrapporter

FOI Memo ”Nättjänster i koalitioner, säkerhetsfrågeställningar – förstudie” [Bengtsson & Westerdahl, 2006] bygger upp den problembeskrivning som i föreliggande rapport återfinns i kapitel 2, Bakgrund. Som underlag redovisas en genomförd enkätundersökning, besvarad av åtta personer från Försvarsmakten/Försvarets materielverk. Förstudien utmynnade i en arkitekturskiss, avsedd att utvecklas i projektet. Skissen beskriver ett webbaserat dokumenthanteringssystem, med rollbaserad åtkomstkontroll.

I rapporten “Publicering i webbapplikationer” [Westerdahl & Bengtsson, 2006] beskrivs de tre grundpelarna – publicering, lagring, sökning – i ett dokumenthanteringssystem för en koalition. Speciellt beskrivs publicerings-rollen. Webbapplikationer diskuteras, speciellt säkerhetsaspekter, till exempel Cross Site Scripting.

Tanken var att fortsätta med en djupare analys av de övriga grundpelarna – lagring och sökning. Detta tonades dock ner, till förmån för koncentrering på rollbaserad åtkomstkontroll till allmänna webbapplikationer, med speciella koalitionsegenskaper. I rapporten ”Access control in a coalition system” [Bengtsson & Westerdahl, 2007] diskuteras detta. Speciellt beskrivs två stycken system som bedömdes lämpliga att utvidga med koalitionsegenskaper. De två systemen är DACS, vilket valdes för utbyggnad, samt GridShib, som används för informationsdelning mellan akademiska institutioner. De två systemens för- och nackdelar jämfördes, till exempel deras åtlydnad av standarder.

I FOI Memo “Access Control in a Web-Based Coalition System, paper with additional comments” [Bengtsson & Westerdahl, 2008] beskrivs det som i föreliggande rapport återfinns i kapitel 3, Resultat. FOI Memot består av två delar, ett konferensbidrag och en del med kommentarer. Kommentarerna är ett avsnitt ”REST versus SOAP”, samt tre kommentarer om säkerhet i DACS. Det senare avhandlar cookies, Single Sign On samt Policy Decision Point.

För projektets räkning har även två examensarbete på D-nivå genomförts. I ”Flexible role-handling in command and control systems” [Landberg, 2006] jämförs tre militära ledningssystem med avseende på hur de hanterar roller och framför allt hur systemen reagerar då roller inte är besatta.

[Falkcrona, 2008] beskriver i ”RBAC and SSO for Web services” problemen med att integrera dynamiska roller med Single Sign-On-system. Här beskrivs även en implementerad referensmodell vilken utgjorde basen för den demonstrator som presenterades ovan.

4 Diskussion

Grundbulten för en koalition mellan parter är ett gemensamt ställningstagande om att man skall samverka och samarbeta. För att realisera detta krävs ett informationssystem som understödjer delning av information inom koalitionen. Aspekten ”need to share” får hög prioritet. Å andra sidan vill den part som tillhandahåller information ha möjlighet att styra hur och vart den förmedlas. Aspekten ”need to know” måste alltså också beaktas. Den inneboende motsättningen mellan dessa aspekter måste kunna hanteras. Slutsatsen är att det i koalitioner är extra viktigt att ha en flexibel åtkomstkontroll, med vars hjälp man kan hitta rätt balans mellan ”need to share” och ”need to know”. Systemet får inte vara låst till ett visst läge.

Det är välkänt att en rollbaserad åtkomstkontroll är lättare att administrera än en individ- eller gruppbaserad. Även detta får extra vikt i koalitioner, eftersom en part inte skall behöva veta i detalj hur en annan part är organiserad.

Det finns flera fördelar med att bygga ett system utifrån kommersiella produkter (COTS) och open source produkter. I koalitionssammanhang är de olika parternas tilltro till systemet viktig. Bedömning av tilltron underlättas och tydliggörs vid användning av standardiserade open source produkter. Dessutom är det helt nödvändigt att följa vedertagna standarder när man skall koppla ihop befintliga system, utvecklade var för sig av de olika parterna.

En koalition innebär att det ställs speciella krav på systemets arkitektur och på dess administration. Systemet bör vara uppbyggt så att det är lätt att inkludera en tillkommande part, likaså att exkludera en avgående part. Varje ingående part bör kunna administrera åtkomstpolicyn för sin tillförda information. Likaså är det önskvärt att varje part kan administrera sina egna användares roller och rättigheter. Det totala systemet bör därför ha en arkitektur som innebär att det är distribuerat och att det möjliggör lokal administration.

Det prototypsystem som byggts inom projektet *Nättjänster i koalitioner, säkerhetsfrågeställningar* beaktar aspekterna ovan. Det är baserat på open source produkten Distributed Access Control System (DACS), som i sin tur baseras på etablerad teknik och standarder. Prototypsystemet har en arkitektur, en federation av lokalt administrerade delar, som väl avspeglar en koalition. Det är emellertid en prototyp, inte ett färdigt system. Exempelvis är administrationen av policies med mera helt manuell, ett grafiskt gränssnitt saknas. Den demonstrerade rollhanteringen behöver utvecklas. En tänkbar utveckling, som dock kräver forskningsinsats, vore att åtkomstkontrollen utnyttjas även inne i delapplikationerna. Det som demonstrerats är en grov åtkomstkontroll, som

huvudsakligen styr anropen till applikationerna. I och med att åtkomstkontrollen anropas enligt etablerad standard, borde det vara möjligt att också anropa den inifrån applikationer. Det krävs dock ytterligare forskning för att belysa om och hur detta är möjligt.

Under projektets gång har det gjorts olika avgränsningar. En sådan avgränsning var att fokusera på en koalitions användning av webbapplikationer. Detta innebär förstås en inskränkning, men det är dock så att fler och fler tjänster byggs med webbteknik. Utvecklingen inom detta område följer två delvis olika linjer. Skillnaden är valet av anrops- och kommunikationsprotokoll, SOAP eller REST. Standardisering ”uppifrån”, via standardiseringsorganisationer och andra sammanslutningar, förordar SOAP. Förenklat kan man säga att detta innebär att internettekniken bara använda för att transportera SOAP-meddelanden. Man definierar sedan ett stort antal nya standarder för hur meddelanden skall se ut för olika tillämpningar, till exempel för samverkande tjänster i affärssystem. REST har å andra sidan utvecklats ”underifrån”, i takt med Internets utveckling. Hårdraget kan man säga att SOAP-arkitekturen passar bäst när man skall nyutveckla ett antal samverkande tjänster, medan REST är mest naturlig för till exempel informationsdelning baserad på internetteknik. REST var det naturliga valet för prototypsystemet, som konsekvens av ovan nämnda aspekter.

5 Referenser

Bengtsson, A., Westerdahl, L. (2008), “Access Control in a Web-Based Coalition System, paper with additional comments”, FOI Memo 2558, 2008-10-13

Bengtsson, A., Westerdahl, L. (2006), ”Nättjänster i koalitioner, säkerhetsfrågeställningar – förstudie”, FOI Memo 1752, 2006-05-31

Bengtsson, A., Westerdahl, L. (2007), ”Access control in a coalition system”, Användarrapport, FOI-R--2393--SE, december 2007

DACS: The Distributed Access Control System
http://dacs.dss.ca/ (2008-12-02)

Falkcrona, J. (2008), ”RBAC and SSO for Web services”, LITH-ISY-EX--08/4107--SE, Linköping 2008-03-20

The Globus Toolkit
http://www.globus.org/toolkit/ (2008-12-03)

GridShib
http://gridshib.globus.org/about.html (2008-12-02)

Higgins, K.J. (2006),"CSRF Vulnerability: A 'Sleeping Giant'", darkReading, 17 oktober 2006
http://www.darkreading.com/security/app-security/showArticle.jhtml?articleID=208804131 (2008-12-02)

Hoffman, B. (2006), “Ajax Security Dangers”, SPI Dynamics, 1 augusti 2006
http://www.sela.co.il/_Uploads/dbsAttachedFiles/AJAXdangers.pdf (2008-12-02)

Landberg, F. (2006), “Flexible role-handling in command and control systems”, LITH-ISY-EX--06/3855--SE, Linköping, 2006-12-04

OASIS (a): Assertions and Protocols for the OASIS, Security Assertion Markup Language (SAML) V2.0, 15 mars 2005
http://docs.oasis-open.org/security/saml/v2.0/ saml-core-2.0-os.pdf (2008-12-02)

OASIS (b): Access Control Markup Language (XACML) version 2.0, 1 februari 2005
http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf (2008-12-02)

O’Reilly, T. (2005), “What Is Web 2.0 - Design Patterns and Business Models for the Next Generation of Software”, O’Reilly, 30 september 2005

http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html (2008-12-02)

Sandhu, R.S., Coyne, E.J., Fernstein, H.L., Youman, C.E. (1996), “Role-Based Access Control Models”, IEEE Computer, vol. 29, no. 2, February 1996, pp. 38-47

Westerdahl, L., Bengtsson, A. (2006), “Publicering i webbapplikationer”, Användarrapport, FOI-R--2142--SE, november 2006

Westerdahl, L. (2008), ”Sammanfattning av Demodag”, FOI Memo 2623, 2008-12-08