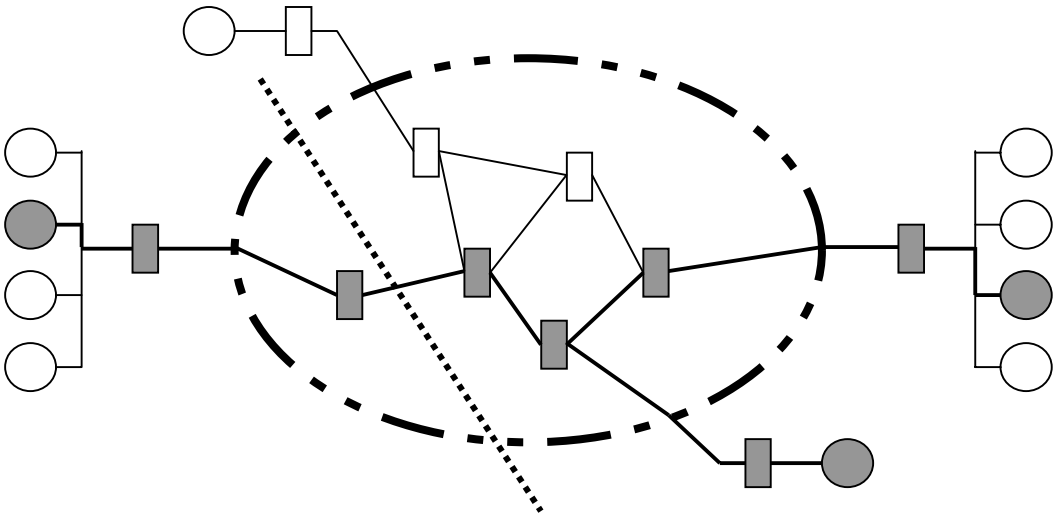
FOI-R--0713--SE
December 2002
ISSN 1650-1942
Användarrapport

Alf Bengtsson

Autentisering med mobila noder och mobil kod - slutrapport



Ledningssystem
581 11 Linköping

TOTALFÖRSVARETS FORSKNINGSINSTITUT

Ledningssystem
Box 1165
581 11 Linköping

FOI-R--0713--SE

December 2002

ISSN 1650-1942

Användarrapport

Alf Bengtsson

Autentisering med mobila noder och mobil kod - slutrapport

Utgivare Totalförsvarets Forskningsinstitut - FOI Ledningssystem Box 1165 581 11 Linköping	**Rapportnummer, ISRN** FOI-R--0713--SE	**Klassificering** Användarrapport
	Forskningsområde 4. Spaning och ledning	
	Månad, år December 2002	**Projektnummer** E7023
	Verksamhetsgren 5. Uppdragsfinansierad verksamhet	
	Delområde 41 Ledning med samband och telekom och IT-system	
Författare/redaktör Alf Bengtsson	**Projektledare** Alf Bengtsson	
	Godkänd av Lennart Nyström	
	Uppdragsgivare/kundbeteckning FM	
	Tekniskt och/eller vetenskapligt ansvarig Alf Bengtsson	

Rapportens titel

Autentisering med mobila noder och mobil kod - slutrapport

Sammanfattning (högst 200 ord)

Föreliggande rapport utgör slutrapport för projektet "Autentisering av mobila noder med mobil kod". Rapporten ger en kort resumé och slutsatser för arbetet under perioden 2000-2002.

Projektet har haft huvudinriktningen autentisering, med tre delinriktningar - autentisering i nätverksbaserade system, ömsesidig användar- och systemautentisering, respektive mobil kod. Dessa har studerats utifrån ett antal krav som ställs av visionen om det nätverksbaserade försvaret.

Tre metoder - biljettbaserade, certifikatbaserade respektive identitetsbaserade - för autentisering i nätverksbaserade system har jämförts. Certifikatbaserade metoder är mest flexibla. Identitetsbaserade metoder kan bara användas i lokala grupper.

En modell för ömsesidig användar- och systemautentisering har tagits fram. Vidare utveckling sker i annat projekt.

Olika typer av mobil programkod har studerats. Mobila agenter är fortfarande inte realiserbara. Mobil kod för styrning i aktiva nät bedöms intressant. Det finns både för- och nackdelar i säkerhetshänseende.

Nyckelord

autentisering, IT-säkerhet, mobil kod, nätverksbaserat försvar

Övriga bibliografiska uppgifter	**Språk** Svenska
ISSN 1650-1942	**Antal sidor:** 26 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization	Report number, ISRN	Report type
FOI – Swedish Defence Research Agency Command and Control Systems P.O. Box 1165 SE-581 11 Linköping	FOI-R--0713--SE	User report
	Research area code 4. C4ISR	
	Month year December 2002	**Project no.** E7023
	Customers code 5. Commissioned Research	
	Sub area code 41 C4I	

Author/s (editor/s)	Project manager
Alf Bengtsson	Alf Bengtsson
	Approved by Lennart Nyström
	Sponsoring agency Swedish Defence
	Scientifically and technically responsible Alf Bengtsson

Report title (In translation)

Authentication of Mobile Nodes and Mobile Code - Final report.

Abstract (not more than 200 words)

The project "Authentication of Mobile Nodes and Mobile Code" ran between 2000-2002. This is the final report with a short summary and conclusions of the project.

The project has focused on authentication in three areas - authentication in network based systems, mutual user and systems authentication and mobile code respectively. These have been viewed from a set of demands given by the vision of the network based defense.

We have studied three methods for authentication in network based systems - ticket based, certificate based and identity based methods respectively. Most flexible are certificate methods. Identity based methods can only be used in local groups.

A model is presented for mutual user and systems authentication. It is further developed in another project.

Different types of mobile code have been studied. Mobile agents are not yet ready for use. Moble code for control of active networks is more likely. We have identified both pros and cons for security.

Keywords

authentication, IT-security, mobile code, network centric defense

Further bibliographic information	Language Swedish
ISSN 1650-1942	**Pages** 26 p.
	Price acc. to pricelist

Innehåll

Figurer

Tabell

1 Inledning

Föreliggande rapport utgör slutrapport för projektet "Autentisering av mobila noder med mobil kod". Rapporten ger en kort resumé med slutsatser för arbetet under perioden 2000-2002.

Projektets inriktning på autentisering, d v s äkthetsbekräftelse och verifiering av identitet, motiveras av att autentiseringen är en hörnsten för att upprätthålla säkerheten i stora system. Speciellt viktig blir den i den typ av system som skall stödja det nätverksbaserade försvaret. De försvarsspecifika kraven - hög mobilitet, dynamisk omkonfigurering, autonomitet m m - ställer autentiseringen inför stora problem. Dessa krav har varit i fokus inom projektet. De har varit vägledande för var och en av tre delinriktningar - autentisering i nätverksbaserade system, ömsesidig användar- och systemautentisering, respektive mobil kod - som funnits i projektet.

De slutsatser som dras i projektet är mycket kort sammanfattade i kapitel 2. I kapitel 3 diskuteras den vision som ligger till grund för ett nätverksbaserat försvar. Utifrån detta formuleras olika krav på ledningssystemet. Kapitel 4 är en resumé med slutsatser inom de tre delinriktningarna - autentisering i nätverksbaserade system, ömsesidig användar- och systemautentisering, respektive mobil kod.

2 Sammanfattande slutsatser

Tre klasser av autentiseringsmetoder jämförs - biljettbaserade metoder, certifikatbaserade metoder respektive identitetsbaserade metoder. De värderas utifrån en lista med krav som har identifierats ur beskrivningar av det nätverksbaserade försvaret. Föga överraskande är den sammanfattande bedömningen att certifikatbaserade metoder bäst uppfyller kravlistan. Dock kan andra metoder vara att föredra i specifika tillämpningar.

Biljettbaserade metoder är beroende av frekvent kontakt med centrala tjänster, vilket försvårar autonomt uppträdande. Förutsedd autonomitet kan hanteras. Däremot är det hög risk för misslyckande vid oförutsedd autonomitet.

Certifikatbaserade metoder har bäst förmåga generellt sett. De kan också kompletteras med metoder som ytterligare ökar förmågan till autonomitet. Bland de certifikatbaserade metoder som analyserats bedöms SPKI/SDSI vara mest flexibel.

Identitetsbaserade metoder är alltför oflexibla för att kunna användas generellt. De kan bara komma ifråga inom lokala grupper.

Tilliten i det totala systemet byggs upp av relationer inom flera kedjor av beroenden mellan komponenter, såväl användare som hård- och mjukvarukomponenter. En modell har tagits fram för dessa beroenden vid användar- och systemautentisering med aktiva kort. Det konstaterade behovet av beroende- och värderingsmodeller medförde att detta arbete har överförts till ett eget projekt.

Mobil kod, d v s programkod som överförs mellan olika noder i det distribuerade systemet, har uppenbara säkerhetskonsekvenser. Men utvecklingen gör att man även i militära system kommer att tvingas ta ställning till mobil kod. Våra slutsatser är att den mest visionära typen av mobil kod, så kallade mobila agenter, inte är mogen för militära system inom överskådlig tid. Vår bedömning är att avgränsad användning av mobil kod kommer att införas, exempelvis för styrning och konfigurering av nät eller datorsystem. Detta innebär ökad komplexitet, med åtföljande säkerhetsfrågor som måste bevakas noggrant.

3 Visionen om ett nätverksbaserat försvar, styrande krav

Försvarsmaktens vision om ett nätverksbaserat försvar har varit vägledande för projektets innehåll. I följande avsnitt redovisar vi hur vi har tolkat visionen, efter diskussioner i referensgrupp och i andra sammanhang. Vi redovisar också vilka av de identifierade kraven som vi huvudsakligen har behandlat.

3.1 Identifierade krav

Kraven på det framtida informations- och ledningssystemet inom försvaret finns inte formulerade i detalj. Detta är naturligt, eftersom en grundtanke är att systemet kontinuerligt skall kunna modifieras i takt med teknikutvecklingen och i takt med att försvarets uppgifter växlar. Detta ger i sig självt ett ytterst väsentligt krav – systemet kan inte vara ett stort, monolitiskt system. Det måste bestå av komponenter och delar, som kopplas ihop via standardiserade gränssnitt, så att det går att modifiera en komponent utan att hela systemet påverkas.

Grundkravet på informations- och ledningssystemet är att det skall användas för att effektivt leda förband i väpnad strid. Det är därför viktigt att systemet följer den doktrin som försvarsmakten har för ledning. Det dokument där denna doktrin sammanfattas är "Försvarsmaktens Grundsyn Ledning" [FM01]. Några citat ur denna kan ge riktlinjer.

"Chefen är ytterst ansvarig för uppgiftens lösande och de beslut som fattas. Detta ansvar kan inte delegeras. Befogenheter tilldelas alltid i paritet med ansvar. Enkla och tydliga ansvars- och lydnadsförhållanden skall eftersträvas."

"Det militära försvarets ledningsmetod är uppdragstaktik."

"Förband i insatsorganisationen skall ha sådan förmåga till självständigt uppträdande att de kan agera i enlighet med överordnad chefs intentioner även om förbindelsen med denne brutits."

"Den framtida striden kommer att ställa allt högre krav på att rätt verkan sätts in, på rätt plats och i rätt tid. Försvarsmaktens vision och strävan är därför utveckling mot så kallad nätverkscentrerad krigföring, med kraftigt förbättrade möjligheter till samordning."

"Chef för insatsstyrka kan tilldelas operativt eller taktiskt ledningsansvar. Vid multinationella insatser kan, med särskilda begränsningar, svenska förband lyda under utländsk chef."

Termen "nätverkscentrerat försvar" är inte närmare definierad i [FM02]. Den innebörd vi lägger i termen är bl a att det inte skall finnas organisatoriska eller tekniska murar som stänger informationsflödet mellan två aktörer som är behöriga till informationen för att lösa en beordrad uppgift. Tekniken skall möjliggöra informationsflöden såväl i en hierarkisk struktur som i en flatare struktur. Kommunikationsfunktionerna skall vara integrerade i ledningssystemet.

Förutom grundkravet, att ledningssystemet skall användas för ledning av väpnad strid, tillkommer flera krav. Det skall stödja försvarets logistik, det skall kunna samverka med civila system mm.

Försvarets uppgifter skall dimensionera systemet. Vilka uppgifter som är aktuella att lösa om 10-20 år går förstås inte att förutspå idag. Men i andra planeringssammanhang bygger man upp målbilder och scenarier baserade på olika kombinationer av de fyra huvuduppgifter som anges idag, enligt Försvarsplan 2000 [FM00]. Det är därför rimligt att fundera över dessa och försöka bedöma respektive huvuduppgifts viktigaste konsekvenser för ledningssystemet.

- VA, Väpnat Angrepp. Den mest tekniktunga uppgiften. I händelse av ett väpnat angrepp skall angriparen kunna mötas över hela det operativa djupet, dvs. Sveriges hela territorium – mark, sjö och luft. Insatsstyrkor, med ledning från rörliga insatsstaber, skall kunna sättas samman av enheter ur alla försvarsgrenar. Sensorer och plattformar skall kunna avläsas och styras på avstånd från de rörliga staberna. För att snabba upp beslutsprocessen skall information kunna överföras mellan olika ledningsnivåer och förband.

  Viktiga konsekvenser av Väpnat Angrepp:

  Kommunikation med hög kapacitet över hela territoriet. Stora mängder information från många olika källor skall vara tillgänglig, för alla som är behöriga, oberoende av förbandsstruktur. Sensor- och plattformsstyrning, skall vara möjlig från ledningsstab. "Små ledningssystem" för insatsstyrkor måste snabbt kunna sättas ihop.

- TI, Territoriell Integritet. Färre sensorer och plattformar och lägre krav på kommunikation över djupet än i uppgift Väpnat Angrepp.

Inga tillkommande konsekvenser jämfört med Väpnat Angrepp.

- II, Internationella Insatser. Försvaret skall kunna bidra till stabiliserande och krisdämpande internationella insatser. Internationell samverkan ställer stora krav på interoperabilitet. Insatsstyrkorna sätts samman av enheter ur flera försvarsgrenar. Ledningen består av central stab, som kan vara placerad i Sverige, samt operativ insatsstab, med rörliga delar, som kan ingå i multinationella stabskonstellationer.

  Viktiga konsekvenser av Internationella Insatser:

  Ett "litet ledningssystem" måste snabbt kunna sättas ihop, liksom i uppgift Väpnat Angrepp. Det som tillkommer är att det skall kunna verka på främmande territorium och med långdistansförbindelse med Sverige. Den mest framträdande konsekvensen av Internationella Insatser är att information skall kunna utväxlas med andra nationers ledningssystem. Detta skall ske på ett så effektivt sätt att samverkansoperationer kan genomföras.

- SS, Stöd till Samhället. Försvarsmakten skall kunna stödja samhället vid t.ex. katastrofer, omfattande terrorism eller grov internationell brottslighet.

  Den mest påtagliga konsekvensen av Stöd till Samhället är kraven på samverkan med det civila samhällets informationssystem. Dessa krav finns också i övriga uppgifter.

Ovanstående axplock ur beskrivningar av försvarsuppgifter och visioner medför ett antal krav på ledningssystemet; krav som är delvis motstridiga. Dessa sammanfattas i följande punktlista. Listan är förstås inte fullständig, men kan likväl tjäna som en kravlista. Som ett allomfattande krav på det framtida ledningssystemet finns "systemet skall vara tillräckligt säkert och robust".

A. Civil teknik och civila system måste användas i högsta möjliga grad. Detta är inte enbart av kostnadsskäl, utan också en konsekvens av uppgifterna. Detta innebär i praktiken att grunden till systemet är framtida Internet-teknik, som på något sätt måste göras "tillräckligt säker". Flexibilitetskrav gör att man skall välja leverantörs- och plattformsoberoende lösningar.

B. Den primära uppgiften hos ledningssystemet är att göra information tillgänglig; på rätt plats, i rätt tid och för rätt aktör. Som sekundär uppgift finns att, under vissa betingelser, möjliggöra

styrning av sensorer och plattformar. Informationen, och styrkommandona, kan vara av olika slag – lägesbilder, order, mobil kod mm.

C. Verksamheten är organiserad i en befäls- och ansvarshierarki. Tekniken i ledningssystemet skall ändock underlätta informationsutbyte oberoende av nivågränser.

D. Informationen skall finnas så nära ägaren (insamlaren) som möjligt. Detta bl.a. för att tydliggöra ansvarsförhållanden.

E. Delar av systemet skall kunna knoppas av, eller på annat sätt sättas upp, vid uppbyggnad av insatsstyrkor, eller vid andra behov av autonoma delsystem.

F. System av system. Bland annat kraven på interoperabilitet och utbyggbarhet gör att det totala systemet måste bestå av delsystem som är hopkopplade via standardiserade gränssnitt.

3.2 Behandlade krav

Projektets innehåll har påverkats dels av kravlistan ovan, dels av vilken kompetens som varit tillgänglig inom IT-säkerhetsgruppen på FOI. Nedan kommenteras vilka av kraven i listan som huvudsakligen har behandlats.

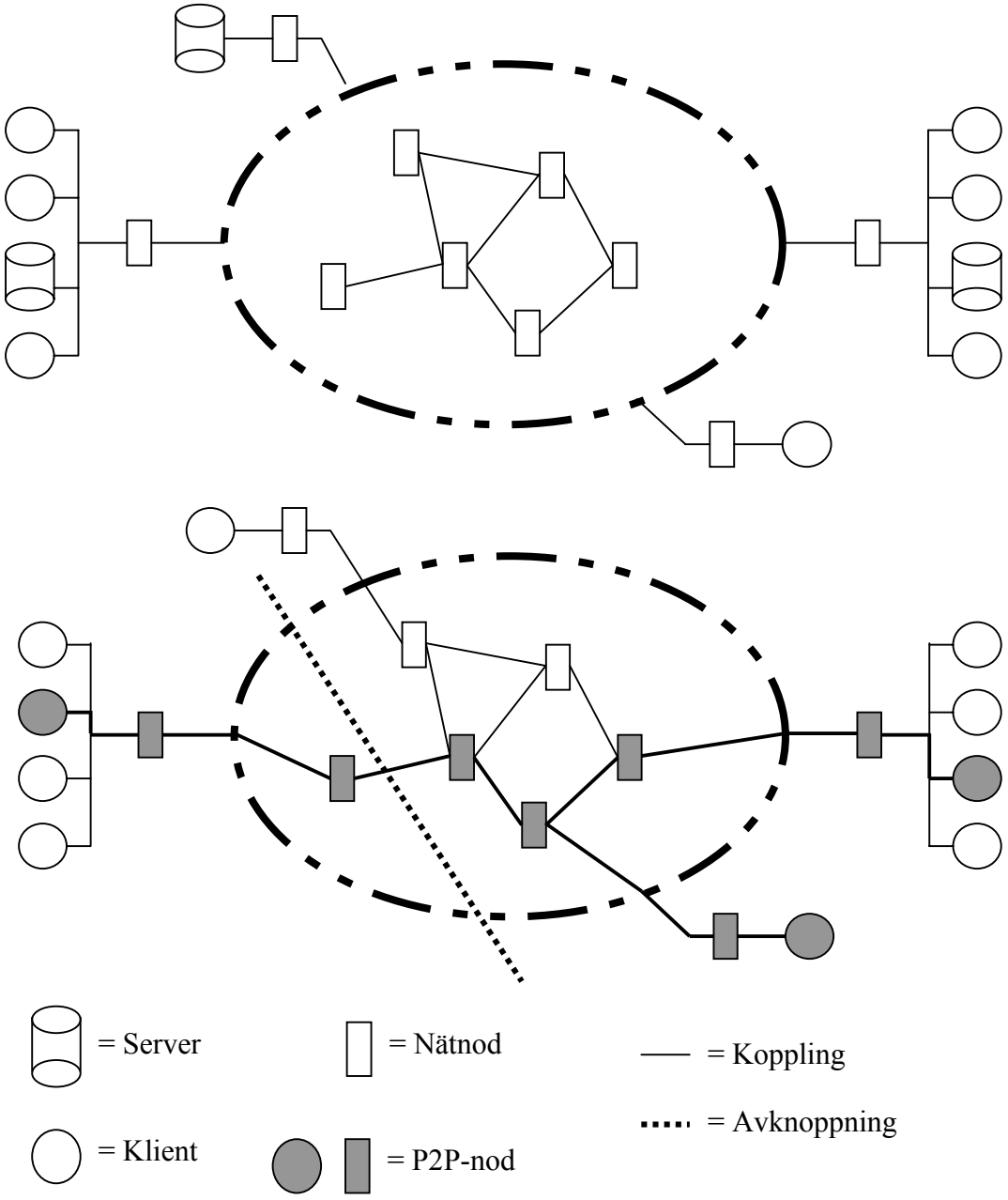
Autentisering, i betydelsen bekräftelse av att en uppgiven identitet verkligen stämmer, är en hörnsten för all IT-säkerhet. Bristfällig autentisering innebär att vissa aktörer kan maskera sig och uppträda i namn av någon annan aktör och då kan självfallet inte önskad säkerhetspolicy upprätthållas. Vi vill påpeka att *aktör* inte bara avser mänskliga användare. Vi har snarare fokuserat på *digitala aktörer* i form av datorer, programkod, radioapparater, sensorer etc.

Autentiseringsfunktionen är en grundbult för samtliga krav A-F. Den är uppenbar för krav B - "rätt aktör". Vi har sett på autentisering för följande krav, sorterade efter omfattning. Kravet E, autonomitet, behandlas i [Ben02]. Det finns också med i [Ben01a] med speciellt fokus på noder med hög mobilitet i delsystemen. I [Ben01b] och [Ben01a] diskuteras C, hierarkiska/icke-hierarkiska system. Civil teknik, A, avhandlas mest i [Ben01b]. Där diskuteras också D, information nära ägaren. Problemen vid koalitioner och andra hopkopplingar, F, återstår att behandla.

Modellering av distribuerade system började vi studera år -00 med inriktning mot ömsesidig användar- och systemautentisering, se [Hal00a] och [Hal00b]. Fokus var på kraven F, system av system, och

på A, civil teknik. Under år -01 genomfördes en förstudie om mer generella möjligheter att modellera och värdera säkerhet i system [Hal01b]. Från och med -02 har denna verksamhet bedrivits i ett nytt separat projekt.

Området mobil programkod har uppenbara konsekvenser för säkerheten. Mobil kod förekommer redan, och kommer att bli allt vanligare, i flera civila system, d v s krav A. Vi började med att studera mobila agenter [Per00] och har sedan avgränsat [Per02] till mobil kod för styrkommandon, krav B.



Figur 3.1 Två olika nättopologier

Schematisk bild av client-server respektive peer-to-peer struktur

4 Resumé och slutsatser

4.1 Autentisering i nätverksbaserade system

Autentisering betyder äkthetsbekräftelse. Metoder för autentisering betyder alltså metoder att verifiera att någonting är äkta. Vi avgränsar till äkthetsbekräftelse av identitet. En aktiv aktör skall kunna verifiera att den identitet som en annan aktör uppger inte är falsk. Vidare avgränsas till "digitaliserade aktörer", t.ex. sensorer, datorprogram, datorer och kommunikationsutrustning. Matchning av fingeravtryck och andra "analoga metoder" att identifiera människor avhandlas alltså inte. Däremot autentiseras även människor ofta via "digitaliserade aktörer", t.ex. aktiva kort.

Digital autentisering tillgår så att en aktör styrker sin identitet genom att bevisa att han besitter en hemlighet, autentiseringsnyckeln. Han använder denna nyckel till att räkna fram någon form av data som presenteras för den andre aktören. Denne har tillgång till en verifieringsnyckel, som han på något sätt vet är knuten till motpartens uppgivna identitet. Han kan med hjälp av verifieringsnyckeln verifiera att de data han mottagit måste ha beräknats med hjälp av rätt autentiseringsnyckel.

Ett oundvikligt steg i alla autentiseringssystem är att objekt med tillhörande identitet måste tillföras systemet, de måste "födas" (och också "dö"). För att man skall kunna ha tilltro till säkerheten måste födelsen övervakas, och styrkas, av någon betrodd aktör, t.ex. en administratör (eller aktörer i samverkan). Ett exempel är att i vissa system tillåts inte aktörerna att själva skapa sina nycklar. En administratör måste skapa nycklarna, och gå i god för att de uppfyller nödvändiga krav. Nycklarna måste sedan på ett säkert sätt överföras till aktören. En viktig fråga är om administratörsrollen kan distribueras till flera administratörer.

Vi har diskuterat frågeställningar, som vi bedömt väsentliga i det komplexa system-av-system som kommer att vara grunden i det nätverksbaserade försvaret.

(a) Hur visar man, på ett säkert sätt, att man besitter autentiseringsnyckeln? Detta är bl.a. de beräkningar med autentiserings- och verifieringsnyckeln som nämndes ovan, samt överföringen av beräkningsresultaten.

(b) Hur knyter man, på ett säkert sätt, ihop en aktörs verifieringsnyckel med hans identitet (annars kan han uppträda under falskt namn)?

(c) Hur löses problemet att en aktör skall kunna agera under olika identiteter (t.ex. i olika roller eller genom olika namngivningssätt i olika delsystem)

(d) Hur hanteras födelseprocessen? Kan denna delegeras, så att autonoma system kan sättas samman?

(e) Hur hanteras dödsprocessen, spärrlistor och andra sätt att spärra ut data (identiteter, nycklar mm) som inte längre är pålitliga.

Autentiseringsmetoder i distribuerade system kan i huvudsak delas in i tre klasser - biljettbaserade, certifikatbaserade respektive identitetsbaserade metoder.

Biljettbaserade, ofta också kallade serverbaserade, system är i huvudsak system, som med hjälp av en, eller flera, central server autentiserar aktörer. En aktör måste inledningsvis logga in på en server, vilken har möjlighet att verifiera om aktören är en giltig användare av systemet som helhet. Därefter begär aktören kortvariga biljetter (sessionsnycklar) av en biljettserver till de tjänster som är av intresse.

Certifikatbaserade system utgår ifrån asymmetriska krypteringsmetoder. Med asymmetri menas att man använder två olika nycklar för signering och verifiering. Signeringsnyckeln är en hemlig nyckel i det avseende att endast en aktör skall ha tillgång och kunna utnyttja denna. Verifieringsnyckeln är publik, vilket innebär att den kan spridas fritt utan att äventyra säkerheten i systemet. Säkerheten i systemet bygger på att det skall vara praktiskt omöjligt att med hjälp av verifieringsnyckeln kunna återskapa signeringsnyckeln och därmed kunna maskera sig som en autentisk avsändare. Vidare är det ett krav att den som vill verifiera en identitet skall kunna vara absolut säker på att den verifieringsnyckel som används tillhör rätt identitet. Denna hopkoppling dokumenteras i ett digitalt (nyckel)certifikat. Det finns även andra typer av certifikat som innehåller information av andra typer än hopkoppling identitet/verifieringsnyckel. Att certifikaten inte är förfalskade verifieras genom att de är digitalt signerade av en betrodd administratör. Den infrastruktur som behövs för att hantera

asymmetriska nycklar och certifikat benämns PKI, Public Key Infrastructure.

En attraktiv tanke är frågan om inte verifieringsnyckeln kan vara lika med identiteten själv. I så fall behövs det ju inga register, certifikat eller annat som kopplar ihop identitet och nyckel. Exempelvis vore det attraktivt att verifiera att ett e-mail kom från uppgiven avsändare genom att som verifieringsnyckel använda t.ex. avsändarens mailadress. Eller att en radionod, som begär access till ett radionät, kan verifieras med hjälp av radions identitet. Dessa metoder benämns identitetsbaserade metoder. Vi vill påpeka att man kan tänka sig att koda in annan information, t ex giltighetstid, i det vi här kallar identitet.

4.1.1 Värdering av autentiseringsklasser

I [Ben01b] beskrivs två eller tre Autentiseringsmetoder för var och en av de tre klasserna. Vi diskuterar för- respektive nackdelar i relation till kravlistan A-F. Föga överraskande fördelar sig för- och nackdelar på sådant sätt att vi inte ville ge en absolut rangordning av de tre klasserna. Nedanstående är direkt citerat ur slutsatskapitlet i [Ben01b].

	Biljett-baserade	**Certifikat-baserade**	**Identitets-baserade**
A Civil teknik	++	+	-
B Informationstillgänglighet	+/-	++	0
C Hierarki	+	++	--
D Informationsägande	-	+	+
E Delsystem	--	+/-	++
F System av system	++	+	--

Tabell 4.1 Värdering av autentiseringsklasser

Bedömningarna med plus och minus ger en fingervisning av vad den övergripande klassen kan klara av, men variationer finns inom klassen. Exempelvis ger certifikatklassen intryck av att vara den mest anpassningsbara modellen, men då skall man ha i åtanke att det finns flera olika implementeringar att välja på och de ger olika resultat. Tabellen är en grov generalisering.

Utifrån detta material bedömer vi att biljettmetoder som Kerberos och certifikatmetoder (PKI) är de kandidater som är mest intressanta för att stödja realiseringen av det nätverksbaserade försvaret.

4.1.2 Autonomitet

Ett av de viktigaste kraven är kravet E på autonomitet hos delsystem. I [Ben02] analyseras de tre klasserna djupare med hänsyn till detta krav. Autonomitet belyses ur fyra aspekter - beroende av globala tjänster, autonomitet förutsedd redan vid design, oförutsedd autonomitet men där initiativet kommer från oss, respektive oförutsedd autonomitet utom vår kontroll (avskärning). Slutsatsen är att certifikatbaserade klassen är att föredra. Speciellt kommenteras att det finns kombinationsmetoder som underlättar autonomitet. Man blir då inte beroende av att certifikat måste signeras av en viss administratör. Man kan i stället tillåta att minst N st vanliga aktörer i samverkan signerar ett certifikat. Nedanstående är direkt citerat ur slutsatskapitlet i [Ben02].

Bedömningarna av de tre autentiseringsklassernas egenskaper vad gäller olika aspekter av autonomitet kan mycket grovt sammanfattas i en tabell.

	Biljettbaserade	Certifikatbaserade	Identitetsbaserade
I. *Beroende av globala tjänster*	Beroende	Starkt beroende i renodlad X.509 Inget beroende i SPKI/SDSI o PGP	Inget beroende
II. *Förutsedd autonomitet*	Kan lösas via segmentering vid systemdesign	Löses väl via segmentering vid systemdesign	Kan lösas på inflexibelt sätt
III. *Oförutsedd men styrd autonomitet*	Kan gå bra under vissa förutsättningar	Löses inflexibelt i X.509 Löses flexibelt i SPKI/SDSI o PGP.	Kan gå bra under vissa förutsättningar
IV. *Oförutsedd ej styrd autonomitet*	Hög risk för misslyckande	PGP flexibelt men primitivt. Risk för misslyckande i de två andra, speciellt X.509. Kombinationsmetoder kan underlätta.	Kan gå bra, men hög risk för misslyckande

Tabell 4.2 Egenskaper vad gäller autonomitet

Bedömningarna ger en fingervisning om egenskaper inom den övergripande klassen, men variationer finns inom klassen. Exempelvis är certifikatklassen den mest anpassningsbara modellen. Man skall då ha i åtanke, att det finns flera olika implementeringar att välja på, och de ger olika resultat. Utifrån vårt material bedömer vi dock att certifikatmetoder (PKI) är de kandidater som är mest intressanta för de krav på autonomitet som finns inom det nätverksbaserade försvaret. Vi anser att SPKI/SDSI är den mest flexibla metoden. En stor nackdel är att den inte är implementerad och testad i samma grad som X.509 och PGP.

4.1.3 Identitetsbaserad autentisering

En av de tre ovan nämnda klasserna är identitetsbaserad autentisering. Dess stora fördel är uppenbar - man slipper register, certifikat el dyl för att koppla ihop verifieringsnyckel med identitet. En miljö där detta är speciellt attraktivt är radiobaserade ad-hocnät. Radiokanalen är en trång resurs och det vore en stor fördel att slippa logistik och kommunikation som beror av register eller certifikat.

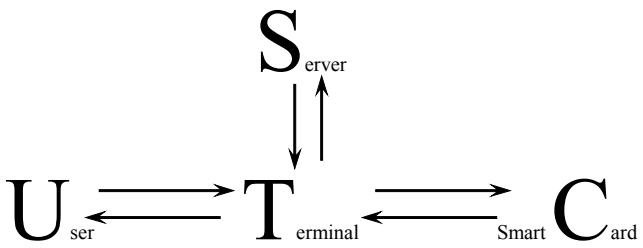
De metoder som finns beskrivna enligt ovan bör övervägas i vissa lokala tillämpningar, t ex radiobaserade ad-hocnät. Den största anledningen till att klassen enligt ovan bedömts som olämplig i generella system är att metoderna inte kan skalas upp till stora system, eftersom samtliga aktörer måste administreras av en och samma administratör.

I [Ben01a] beskrivs en metod som kunde löst skalningsproblemet. Om administratörerna kan organiseras i en hierarki, vilket ofta är fallet i militära system, kan administrationen delegeras. Metoden, patenterad av FOI, bygger på att nycklar genereras top-down i hierarkin. Tyvärr kan den inte göras säker med de två algoritmer, exponentiering i ett ändligt fält respektive multiplikation av punkter på elliptisk kurva, som beskrivs i [Ben01a]. Två aktörer i maskopi kan tillsammans beräkna en hemlighet tillhörande en nod på en högre nivå i hierarkin.

4.2 Ömsesidig användar- och systemautentisering

Inom ramen för denna aktivitet har behoven av och möjligheterna med förbättrad verifiering av användares identitet, dvs användarautentisering, studerats. Arbetet utgick från vad som kan åstadkommas med aktiva kort. Förutom att stärka autentiseringen av användare möjliggör aktiva kort också effektiv autentisering av system, dvs användare kan med hjälp av kortet kontrollera att systemet är äkta.

För att kunna analysera säkerheten hos ett autentiseringssystem baserat på aktiva kort behövs en modell som inkluderar både de inblandade enheterna och kommunikationen mellan dessa. En modell som uppfyller dessa krav tillsammans med en analys av potentiella presenteras i [Hal00a]. För att ytterligare förbättra förutsättningarna för en säkerhetsanalys introduceras en utvidgad modell. Denna modell tydliggör två problem i autentiseringssystem baserade på konventionella aktiva kort. För det första passerar all information terminalen, vilken är den enhet vars integritet är svårast att säkerställa. Vidare saknas ett gränssnitt för direkt kommunikation mellan kortet och användaren. Figuren nedan visar hur informationen flödar mellan de enheter vilka är inblandade i en autentiseringsprocess baserad på konventionella aktiva kort. Figuren illustrerar därmed också de två dominerande säkerhetsproblemen hos sådana system, vilka beror på att terminalen och inte det aktiva kortet utgör navet i informationskedjan. Med anledning av detta behövs säkerhetshöjande förbättringar. I [Hal00a] beskrivs möjliga implementationer av sådana förbättringar. Detta arbete har också presenterats på den vetenskapliga konferensen Medinfo 2001 [Hal01a].



Figur 4.1 Informationsflödet mellan enheter vid autentisering

I [Hal00b] diskuteras möjligheterna att skapa en struktur för validering av terminalers integritet. Denna struktur skulle utgöra den nödvändiga infrastrukturen för olika metoder vilka stöder valideringen av terminalintegritet. Det växande beroendet av informationssystem leder till att vi överför förmågor, som till exempel att signera dokument, och viktiga data till dessa system. Därmed måste vi kunna lita på att den överförda informationen hanteras korrekt. Autentisering och validering av integriteten är viktiga processer för att bygga upp detta förtroende. Eftersom säkerheten hos olika komponenter (såsom program och systemrutiner) varierar, finns ett behov av att kunna begränsa vilka komponenter som kan användas i en given situation. Därmed måste tilliten till enskilda komponenter kunna bestämmas, vilket

kräver att både ursprunget och integriteten beaktas. För detta ändamål kan elektroniska signaturer nyttjas, eftersom de kan användas för att kontrollera både en komponents ursprung, dvs vem som har signerat den, och att den inte har modifierats efter att den signerades. För att kunna verifiera olika aktörers signaturer måste certifikat för dessa utfärdas av en central auktoritet. Dessa certifikat kan då också innehålla en värdering av förtroendet för den aktuella aktören. Det finns alltså ett antal parametrar som kan användas för att bedöma vilken tilltro olika system ska tillmätas vid olika tidpunkter.

En slutsats av det ovan beskrivna arbetet är att det finns ett stort behov av att kunna designa system för att från början innehålla de mekanismer som krävs för att uppfylla ställda säkerhetskrav. Funderingar kring detta resulterade i den problembeskrivning som krävdes för deltagande i workshopen Information Security System Scoring and Ranking (ISSSR), 21-23 maj 2001. ISSSR resulterade i ett dokument som har publicerats av Applied Computer Security Associates (ACSA) [Hal01b] . Vidare har insynen lett till formuleringen av det avknoppade projektet ”Kvantifiering av säkerheten i distribuerade informationssystem”, vilket har startats under 2002.

4.3 Mobil kod

Mobil kod är en sammanfattande benämning på programkod eller andra styrkommandon som skapas på ett ställe i ett distribuerat system men som exekveras och/eller tolkas på ett annat ställe. Olika varianter av mobil kod finns redan, och kommer att bli allt vanligare, i mängder av civila standardsystem. Exempel är makrokommandon i textdokument, scripts och applets i webbsidor m fl, m fl. Det är uppenbart att det är stora säkerhetsproblem med mobil kod. Det finns ju också flera exempel på illasinnad mobil kod - virus, maskar, trojaner etc.

I grova drag kan man beskriva säkerhetshanteringen av mobil kod som ett tvåstegsförfarande. Steg 1 innebär en absolut säker autentisering (jfr ovan) av kodens ursprung, såväl var koden ursprungligen skapades och/eller modifierades, som vilken nod som närmast sände iväg koden. Steg 2 innebär en uppsättning restriktioner, baserade på data från steg 1, över vad koden tillåts göra. Man brukar bildligt kalla detta för en sandlåda, inom vilken koden skall hållas. I [And01] beskrivs detta för JavaScript, tidigare har det beskrivits för Java och för andra system i Unix- och Windowsmiljö.

En första fråga att ställa är om mobil kod över huvud taget skall få förekomma i militär miljö. Det är dock så att med det tydliga kravet på att bygga på civil teknik, krav A i kap 3.1, kommer man snart att tvingas ta ställning till system som innehåller mobil kod. Dessutom finns det försvarsspecifika tillämpningar för mobil kod. Exempel är styrning av sensornät, möjlighet att utnyttja intermittent samband m m.

Den mest visionära varianten av mobil kod är s k mobila agenter. Dessa består av kompletta program som självständigt tar beslut om att förflytta sig till andra noder i nätet. Maskar kan sägas vara illasinnade mobila agenter. Nyttiga mobila agenter kan utföra exempelvis datainhämtning av olika slag. I [Per00] beskrivs prototyper och arkitektur för mobila agenter. Slutsatsen, bl a baserad på konferensdeltagande, är att mobila agenter en tid framöver är en omogen teknik.

I [Per01] avhandlas aktiva nät, vilket är en speciell tillämpning av mobil kod. Man utnyttjar mobil kod till att under drift modifiera funktionaliteten i nätverksnoder. Små steg i denna riktning är redan tagna, t ex konfigurering av brandväggar. En framtida möjlig, säkerhetshöjande, tillämpning kan vara att vid detekterad Denial of Service-attack snabbt anpassa paketfiltrering i ett stort antal nätverksnoder. I [Per02] beskrivs en speciell prototyp, ANTS, för aktiva nät. Den är implementerad och har använts för experiment vid FOI. Slutsatsen är att eftersom den använder Javas sandlåda är vissa säkerhetskrav uppfyllda. Den största bristen rör autentisering av den mobila koden.

7 Referenser

[And00] Andersson C, "Säkerhetsbrister i JavaScript", Underlagsrapport FOI-R--0124--SE, juni 2001, FOI.

[Ben00] Bengtsson A, Hallberg J, Lindahl D, Lindbergh U, Persson M, "Tillämpad nätverkssäkerhet", Underlagsrapport FOA-R--00-01472-505--SE, mars 2000, FOI.

[Ben01a] Bengtsson A, "An attempt to get identity-based authentication and certification in a hierarchic tree", Scientific report FOI-R-0114--SE, March 2001, FOI.

[Ben01b] Bengtsson A, Hunstad A & Westerdahl L, "Autentisering i nätverksbaserade system", Användarrapport FOI-R--0331--SE, December 2001, FOI.

[Ben02] Bengtsson A, Hunstad A & Westerdahl L, "Autonomitet vid autentisering i nätverksbaserade system", Användarrapport FOI-R--0xxx--SE, December 2002, FOI.

[FM00] Försvarsplan 2000

[FM01] Försvarsmaktens grundsyn ledning 2001, Stockholm, FM 2001, 28 s.

[FM02] Försvarsmaktsidé 2020, Rapporterna 1-6, Årsrapporter från perspektivplaneringen Stockholm, Försvarets bok- och blankettförråd.

[Hal00a] Hallberg J, "Secure User and System Authentication - Beyond Conventional Smart Cards", Scientific report FOA-R--00-01495-505--SE, February 2000, FOI.

[Hal00b] Hallberg J, "Terminal Security Verification in Smart Card-Based Authentication Systems", Scientific report FOA-R--00-01714-505--SE, December 2000, FOI.

[Hal01a] Hallberg J, Hallberg N, and Timpka T. Towards second-generation smart card-based authentication in health information systems: the secure server model. In V.L. Patel, R. Rogers, and R. Haux. Proceedings of the 10th World Congress on Medical Informatics. (2001) pp. 1257-61.

[Hal01b] `http://www.acsac.org/measurement/`

[Per00] Persson M, "Mobile Agent Architectures", Scientific report FOA-R--00-01700-503--SE, December 2000, FOI

[Per01] Persson M, "Säkerhet i aktiva nät", Användarrapport FOI-R--0309--SE, December 2001, FOI.

[Per02] Persson M, "Beskrivning av ANTS och dess säkerhetsbrister", FOI Memo FOI-----SE, December 2002, FOI