Handbok Totalförsvarets Signalskyddstjänst

Grundläggande regler för signalskyddstjänsten

HTST Grunder

TSA

2007

Handbok Totalförsvarets Signalskyddstjänst

Grundläggande regler
för signalskyddstjänsten

H TST Grunder

Central lagerhållning:
Försvarets bok- och blankettförråd

FÖRSVARSMAKTEN 2007-04-27 12 839:63626
HÖGKVARTERET TFD

Handbok totalförsvarets signalskyddstjänst, grundläggande regler för signalskyddstjänsten (H TST Grunder), 2007 års utgåva, M7746-734002 fastställs för tillämpning inom totalförsvaret fr o m 2007-07-01

H TST Grunder 2007 ersätter H TST Grunder 2001 M7746-734001 som därmed upphör att gälla.

Håkan Pettersson

John Daniels

Boken är publicerad i samarbete med
Mediablocket AB
Tryck Elanders Tofters AB
Foto Johnny Davidsson
Clipart från CorelDraw
M7746-734002

FÖRORD

I 4 § förordningen (2000:555) med instruktion för Försvarsmakten (FM) framgår att Försvarsmakten skall leda och samordna signalskyddstjänsten inklusive arbetet med säkra kryptografiska funktioner inom totalförsvaret. I 39 § samma förordning framgår att FM får meddela övriga statliga myndigheter föreskrifter i frågor om signalskyddstjänsten inklusive säkra kryptografiska funktioner.

Verkställande organ för FM ledning och samordning är totalförsvarets signalskyddssamordning (TSA) som är en funktion inom säkerhetskontoret (SÄKK) vid militära underrättelse- och säkerhetstjänsten (MUST) i Högkvarteret (HKV). Begreppet ”TSA” kommer i denna handbok genomgående att användas när ”funktionen för totalförsvarets signalskyddssamordning” åsyftas.

Signalskydd kan beskrivas som telekommunikationernas (logiska) säkerhetsskydd, därmed är signalskyddstjänsten starkt knuten till såväl sambandstjänsten som till säkerhetstjänsten.

Föreskrifter och allmänna råd för signalskyddstjänsten inom totalförsvaret syftar till att få ett väl fungerande signalskydd genom användning av säkra kryptografiska funktioner, varigenom långvariga och dolda skadeverkningar för rikets säkerhet och krisberedskap undviks.

Föreskrifterna för totalförsvarets signalskyddstjänst är utgivna i försvarets författningssamling (FFS 2005:2).

Föreskrifterna i denna författning gäller för statliga myndigheter.

1 § FFS 2005:2

Försvarsmakten får medge undantag från Försvarsmaktens föreskrifter om signalskyddstjänsten inom totalförsvaret.

Överbefälhavaren eller den han bestämmer fattar beslut i ärenden om undantag.

47 § andra stycket FFS 2005:2

Föreskrifterna ingår också tillsammans med allmänna råd i H TST Grunder. Föreskrifterna i H TST Grunder är markerade med grön bakgrund. Föreskriftens paragraf- och styckenummer anges i direkt anslutning till föreskriften.

H TST Grunder riktar sig till personal som planlägger, leder och samordnar signalskyddstjänsten samt till den personal som nyttjar, betjänar eller på annat sätt handhar signalskyddssystem. H TST Grunder riktar sig också till den personal som utvecklar, anskaffar, underhåller, förrådshåller och avvecklar signalskyddsmateriel.

Innehåll

Definitioner

För att förstå och rätt tolka innebörden av de föreskrifter och allmänna råd som återges i denna handbok tillämpas följande definitioner enligt Försvarsmaktens föreskrifter om signalskyddstjänsten inom totalförsvaret 3 § FFS 2005:2. Observera att en fullständig sammanställning av de inom signalskyddstjänsten vanligast förekommande begreppen återfinns i bilaga 11.

1. ***IT-system**: system med teknik som hanterar och utbyter information med omgivningen,*

2. ***kryptografisk funktion**: metoder och principer för*
   - *skydd av information mot insyn vid överföring och lagring med hjälp av kryptering,*
   - *identifiering och autentisering, och*
   - *signering och verifiering av information,*

3. ***signalskyddssystem**:*
   - *system med kryptografiska funktioner som är godkänt av Högkvarteret, och*
   - *system för skydd mot signalunderrättelsetjänst, störsändning eller falsk signalering som är godkända av Högkvarteret,*

4. ***Högkvarteret**: Försvarsmaktens högkvarter,*

5. ***signalskyddsmateriel**: kryptoapparat, komponent eller utrustning som innehåller kryptomodul eller krypteringsfunktion samt annan signalskyddsspecifik materiel eller signalskyddsspecifik programvara som används eller avses användas i ett signalskyddssystem,*

6. ***enhet**: en myndighets organisatoriska enheter, såsom central ledning, regionala och lokala enheter,*

7. ***signalskyddstjänst**: verksamhet som syftar till att förhindra obehörig insyn i och påverkan av telekommunikationer, samt användning av kryptografiska funktioner i IT-system,*

8. ***aktivt kort**: kort utgivna av Högkvarteret som har försetts med någon av följande beteckningar:*
   a) Totalförsvarets Aktiva Kort (TAK),
   b) Totalförsvarets Elektroniska ID-kort (TEID), eller
   c) Totalförsvarets Nyckelbärarkort (NBK),

9. ***kvitto för aktivt kort**: handling som innehåller nödvändiga data för redovisning och hantering av ett aktivt kort,*

10. ***signalskyddsincident**: när en kryptonyckel har eller kan antas ha röjts (nyckelincident) eller när signalskyddsmateriel saknas eller kan antas ha manipulerats (materielincident),*

11. ***kryptonycklar**:*
    – *kryptonycklar,*
    – *systemnycklar,*
    – *täcknycklar,*
    – *anropsnycklar,*
    – *lösennycklar,*
    – *autentiseringsnycklar, och*
    – *frekvenshoppsnycklar,*
    som omfattas av sekretess enligt sekretesslagen (1980:100),

12. ***signalskyddspersonal**: signalskyddschef, biträdande signalskyddschef, systemoperatör, nyckeladministratör och kortadministratör,*

13. ***signalkontroll**: kontroll av signalskyddet i telekommunikations- och IT-system i syfte att klarlägga dels riskerna för obehörig åtkomst eller störande eller manipulering av data, dels att systemen används enligt gällande regler, samt kontroll av röjande signaler (RÖS),*

14. ***nyckelansvarig****: myndighet, och i förekommande fall dess enheter, som administrativt och operativt ansvarar för en viss kryptonyckelserie,*

15. ***hemlig****: uppgift som anges i 4 § 1 säkerhetsskyddsförordningen (1996:633),*

16. ***hemlig signalskyddsmateriel****: signalskyddsmateriel som innehåller sådan uppgift som anges i 4 § 1 säkerhetsskyddsförordningen.*

Kapitel 1
Hot mot telekommunikations- och IT-system

För det militära försvaret och hotbildsbeskrivningar, se Telekrig 1997 Lärobok för armén (M7746-168001).

Hot mot våra telekommunikationer har alltid förekommit i form av signalspaning, störsändning och falsk signalering. Traditionellt sett kommer hoten från främmande makts organisationer, t ex signalunderrättelsetjänst där det i fredstid främst gäller strategisk signalunderrättelsetjänst som syftar till att söka upplysningar för att kunna kartlägga vårt totalförsvar samt att identifiera sårbarheter i samhället.

Vid beredskapshöjningar och vid krig som berör vår världsdel förstärks signalunderrättelsetjänsten. Kapaciteten för insamling och bearbetning ökas. Spaningen blir då av en mer operativ karaktär och inriktas till största delen mot huvudmotståndarens telekommunikationssystem. Förutom signalspaning tillkommer även störsändning som syftar till att hindra eller försvåra vår användning av telekommunikationer samt falksignalering som syftar till att skaffa underrättelser, vilseleda eller förvirra ledningen och fördröja kommunikationen.

I dagligt tal inom IT-säkerheten används normalt sett andra begrepp än signalspaning, störsändning och falsk signalering. För mer information se H SÄK IT Hot.

Eftersom vi idag har en omfattande infrastruktur av datanätverk, såsom Internet och LAN (Local Area Network – lokalt nätverk), och vi i stor omfattning är beroende av flertalet IT-system är signalunderrättelsetjänsten anpassad för att även kunna inhämta underrättelser ur dessa. Även metoder och system för störsändning och falsk signalering är utvecklade och utgör en del i begreppet informationsoperationer. Då allt fler samhällsviktiga system är beroende av IT, t ex elförsörjning och kommunikation har samhällets sårbarhet ökat.

Vi har fått nya typer av ”aktörer” som utgör hot mot våra telekommunikations- och IT-system, från en enskild hacker till terroristorganisationer. Denna typ av hot, som tidigare hänfördes till krigshandlingar, är nu en realitet i fredstid även för enskilda personer.

I H TST Grunder behandlas endast de telehot mot våra telekommunikations- och IT-system som föreligger i form av avsiktlig eller oavsiktlig obehörig insyn och påverkan genom avlyssning (signalspaning), störsändning samt falsk signalering.

Varje myndighet skall se till att den personal som nyttjar, betjänar eller på annat sätt hanterar telekommunikations- och IT-system har kunskap om hur dessa system kan hotas genom avsiktlig eller oavsiktlig obehörig insyn eller påverkan.

2 § FFS 2005:2

1.1 Avlyssningshot

Avlyssning genom signalspaning pågår ständigt mot vårt lands telekommunikations- och IT-system. Detta är en väsentlig del av främmande makts underrättelsetjänst. Den bedrivs med förhållandevis riskfria insatser och kan ge mycket bra resultat. Signalunderrättelsetjänst bedrivs på strategisk, operativ och taktisk nivå.

Det är av särskild vikt att svensk personal beaktar riskerna med avlyssningshotet när Sverige deltar i internationell verksamhet.

Syftet med signalspaning är att få insyn i vår verksamhet för att inhämta underrättelser genom att upptäcka, avlyssna, kapacitetsbestäm-

ma och lägesbestämma våra telekommunikations- och IT-system. Signalspaning kan ske från vårt territorium, andra länders territorium, internationellt vatten och luftrum samt från rymden.

Främmande underrättelsetjänst visar ett påtagligt intresse för våra prov och försök. Särskilt intressant är materiel som är under utveckling eftersom dessa prov och försök ger goda möjligheter att tidigt få kunskap om materiel redan innan den har tagits i operativt bruk. Främmande underrättelsetjänst visar även stort intresse för våra ledningsövningar samt vårt deltagande i internationell verksamhet.

Främmande signalunderrättelsetjänst, riktad mot våra intressen såväl nationellt som internationellt, syftar till att öka kunskapen om vårt samhälle. Detta sker genom inhämtning och bearbetning av uppgifter om:

- telekommunikations- och IT-system,
- kommunikations- och IT-systemens störtålighet,
- infrastrukturens störtålighet,
- åtgärder för försörjning,
- organisation,
- operativa och taktiska förberedelser,
- materiel,
- skyddsobjekt,
- beredskapsförhållanden,
- krishantering,
- industrier samt
- krigsplanläggning.

Genom signalunderrättelsetjänst i fred säkerställer främmande makt underlag för att, i krig, kunna utföra signalspaning, störsändning och falsk signalering, samtidigt som våra fredsförhållanden och beredskapsförändringar fortlöpande klarläggs.

Främmande signalunderrättelsetjänst i krig inriktas främst på att söka operativa och taktiska underrättelser. I fredstid kan även främmande underrättelsetjänst, terroristorganisationer samt hackers störa och göra intrång i våra telekommunikations- och IT-system i syfte att klarlägga och utnyttja eventuella brister i våra system.

1.1.1 Medel och metoder

Teknisk signalspaning bedrivs med syftet att klarlägga tekniska egenskaper hos system som nyttjar elektromagnetiska vågor. Signalspaning mot kommunikation syftar till att inhämta underrättelser ur våra telekommunikations- och IT-system.

Det bedöms att signalspaning i fred sker från främmande makts territorium, från internationellt vatten och luftrum, från satelliter samt från vårt eget territorium.

I krig utförs signalunderrättelsetjänst även med hjälp av taktiska signalspanings- och televapenförband. Taktisk signalspaning har en kortsiktig inriktning som syftar till att upptäcka vårt utnyttjande av det elektromagnetiska spektrumet och omfattar sökning, detektering, mätning, lokalisering, analysering, klassificering och identifiering av våra signaler.

Signalunderrättelsetjänstens möjligheter att nå resultat är beroende av de överföringssätt som används vid vår kommunikation, av den tid under vilken överföringen pågår och av den sammanlagda trafikmängden. Resultatet påverkas också av de övriga signalskyddsåtgärder som vidtas.

Sändning på LF (30–300 KHz), MF (300–3000 KHz) och HF (3–30 MHz) som har en räckvidd som vida överstiger vårt lands gränser kan avlyssnas från främmande territorium, varifrån sändarna också kan pejlas. Dessa frekvensområden kallas även Lång-, Mellan- och Kortvåg.

Sändning på ultrakortvåg – benämns även VHF (30–300 MHz) och UHF (300–3000 MHz) – kan avlyssnas och pejlas på avstånd upp till 150 kilometer. Från flygplan och satelliter kan avlyssning och pejling ske på avsevärt större avstånd. Dessutom kan särskilda förhållanden för vågutbredning på den lägre delen av VHF-bandet (30–150 MHz) medföra stora avlyssningsavstånd (upp till 400 mil, dock ej kortare än cirka 50 mil). Dessa fenomen brukar kallas E-skip eller E_S och förekommer främst på senvåren och sommaren. E-skip uppträder när som helst på dygnet men förekommer oftast mitt på dagen samt mellan klockan sex och åtta på kvällen. I detta sammanhang bör påpekas att vissa typer av mobil radio, exempelvis Mobitex och Ra 180/480,

nyttjar den lägre delen av ultrakortvågsbandet, varför den då är enkel att avlyssna och pejla på mycket stora avstånd.

Positionering (pejling) av mobiltelefoner kan även utföras av mobiloperatören genom att denne jämför signalstyrkor och tidsinformation från ett flertal basstationer som står i kontakt med mobiltelefonen. Positionering kan ske då telefonen är påslagen, även när den ej används för samtal. Detta är särskilt viktigt att beakta vid vistelse utomlands då vi kan förutsätta att främmande makts signalunderrättelsetjänst får denna information från det egna landets mobiloperatörer.

Radiolänkförbindelser inom ultrakortvågs- och mikrovågsbandet (SHF och EHF – 3–300 GHz) är möjliga att avlyssna. Normalt sker avlyssning i sändarantennens huvudlob, där den starkaste signalen finns. Avlyssning kan även ske i de svagare sido- och backloberna.

Avlyssning från satelliter kan ske av ultrakortvågsbandet och uppåt. Fördelen med avlyssning från satelliter är att radiovågors utbredningsdämpning, i fri rymd, är väldigt liten. Detta möjliggör avlyssning av kommunikation med låg sändareffekt (<1 watt), som längs med markytan, har en normal räckvidd på ett fåtal kilometer.

En annan metod för avlyssning är att placera en fjärrstyrd radiomottagare i närheten av en sändare. Den som avlyssnar kan, geografiskt, befinna sig var som helst och styra sin mottagare via exempelvis Internet.

Förbindelser på kabel (tråd och optofiber) är i allmänhet svårare att avlyssna än radioförbindelser, eftersom avlyssning i regel kräver inkoppling på förbindelsen. I telenät nyttjas dock både tråd-, radio- och radiolänkförbindelser, vilket innebär att risken för avlyssning är lika stor som för radioförbindelser.

Bredbandsanslutningar över det ordinarie elnätet är möjliga att avlyssna på avstånd upp till flera hundra meter. Detta beroende på att elnätet ej är anpassat för att överföra dessa snabba datorförbindelser, vilket i sin tur innebär att kraftledningar och motsvarande fungerar som sändarantenner.

Optiska eller hydroakustiska förbindelser har normalt så små räckvidder att de är undantagna systematiserad signalspaning. Vid optisk signalering under mörker samt vid hydroakustisk signalering då skikt-

ningar i vatten förorsakar onormala vågutbredningsförhållanden kan dock räckvidderna bli sådana att avlyssning är möjlig.

Tele- och datakommunikation som skickas över externt nätverk, t ex Internet kan avlyssnas genom avtappning av de nätkomponenter i knutpunkter som förmedlar kommunikationen. Avtappningen kan ske fysiskt genom inkoppling och logiskt genom omstyrning av kommunikationen.

Radio-LAN (WLAN) är radiobaserade nätverk som sänder på frekvensområdena 2.4 och/eller 5 GHz. Dessa nätverk kan enkelt avlyssnas på flera hundra meters avstånd. Med, för ändamålet, särskilt anpassade mottagare och antenner kan avlyssningsavståndet ökas avsevärt.

Tele- och datakommunikation mellan telefonväxlar, datorer (klienter) och servrar som befinner sig i Sverige kan utan vår vetskap förmedlas genom ett antal länder innan det når sin slutdestination.

Bluetooth är namnet på radiobaserad anslutning mellan exempelvis mobiltelefon och dator. Bluetooth finns idag i praktiskt taget alla nya mobiltelefoner och bärbara (hand-) datorer och är tänkt att användas som ersättare av traditionella kabelanslutningar.

Radiosändning över Bluetooth sker på 2.4 GHz och har en ungefärlig räckvidd på 10 eller 100 meter beroende på vilken klass av Bluetooth som används. Med, för ändamålet, särskilt anpassade mottagare och antenner kan avlyssningsavståndet ökas avsevärt.

Många Bluetooth-utrustade enheter har som grundinställning att tillåta vem som helst att ansluta till enheten utan någon som helst form av autentisering. Detta möjliggör för obehöriga att exempelvis läsa ut handdatorns kalenderdata eller mobiltelefonens telefonbok. Krypteringen i Bluetooth är inte godkänd för att skydda hemliga uppgifter.

Med hjälp av särskilda dataprogram kan våra klienter och servrar lägesbestämmas. Metoden kallas routetracing och dataprogram för detta finns lätt tillgängliga på Internet.

Elektronisk utrustning som ingår i telekommunikations- och IT-system kan alstra icke önskade elektromagnetiska eller akustiska signaler, som kan bidra till att sekretessbelagd information röjs om signalerna kan avlyssnas och tydas av obehörig. Dessa benämns röjande signaler

(RÖS). Möjligheterna att avlyssna RÖS kan bedömas som goda, speciellt mot permanenta platser. RÖS kan exempelvis utgöras av:

- Video-rös: Signaler från bildgenererande komponenter i datorutrustning. Dessa kan uppfattas trots att bildskärmen är frånslagen.
- Tecken-RÖS: Signaler från t ex tangentbord till dator.
- Radio-RÖS: Signaler som överlagras på signal från radioutrustning med näraliggande placering

Skydd mot RÖS-avlyssning kan ske genom att använda RÖS-skyddade apparater, RÖS-skyddade rum och kabinett, utnyttja naturliga skydd i omgivningen eller genom att tillämpa ett säkerhetsavstånd till obevakat område. För att skydda tekniska system mot informationsläckage genom RÖS utges inom Försvarsmakten Försvarsmaktens RÖS-policy.

1.1.2 Bearbetning

Främmande signalunderrättelsetjänst bearbetar insamlad information genom text-, trafik- och teknisk bearbetning.

Textbearbetning syftar till att ta fram underrättelser ur inhämtad klartext och forcerad kryptotext.

Trots att syftet med kryptering är att göra texten oläslig för utomstående så har historien visat att detta i många fall har misslyckats, kryptot har forcerats. Ofta är orsaken en felaktig hantering. Att bedöma ett kryptosystem och utfärda regler för dess användning är således en grannlaga och mycket viktig uppgift.

Trafikbearbetning syftar till att utvinna underrättelser ur telekommunikationens trafikbild. Denna kan bestå av frekvenser, pejlbäringar, anropssignaler, telefon- och faxnummer, IP-adresser samt kommunikationens volym, vägar, intensitet, metoder samt förekomst av krypto- och klartexter.

Trafikbearbetning kan resultera i detaljerade underrättelser om vår organisation, verksamhet, geografisk placering, kapacitet, beredskap och avsikt samt ge kännedom om våra system.

Teknisk bearbetning av mottagna signaler syftar till att ge kunskap om vår materiels tekniska utformning, egenskaper och om dess användning för att därigenom skapa underlag för informationsoperationer.

1.2 Övriga telehot

1.2.1 Störning

Störsändning syftar till att negativt påverka ledningsförmågan genom att störa ut vissa frekvensområden, enskilda frekvenser, enskilda förbindelser, funktioner eller enheter inom visst geografiskt område.

Smalbandig störsändning (störning av en kanal åt gången) bedöms i huvudsak komma att sättas in mot våra radioförbindelser. Verkan av störsändningen beror på störningens signalstyrka vid mottagarantennen i förhållande till den önskade signalen.

Effektiv störsändning mot våra radiolänksignaler inom högre frekvensområden är svårare att genomföra än i lägre frekvensområden där störsändning även kan ske i sido- och baklober.

Störning kan ske såväl från fasta anläggningar såsom rörliga plattformar i form av fordon, fartyg och luftfartyg.

Engångsstörsändare är batteridrivna störsändare som har relativt låg uteffekt och en begränsad driftstid. Dessa störsändare kan dock ge stor störverkan då de kan placeras ut i närheten av det tänkta störmålet med hjälp av artilleri eller genom att de släpps från flygplan.

Till kategorin störning hör även så kallade Denial of Service- (DoS) attacker som är en vanlig företeelse på Internet. En DoS-attack kan exempelvis utföras genom att angriparen ”bombarderar” en nätverksansluten utrustning med ett mycket stort antal uppkopplingsförfrågningar per sekund, varpå den angripna utrustningen blir så hårt belastad att den slutar att fungera.

Den vanligaste formen av DoS-attack kallas Distributed DoS (DDoS), där angriparen utnyttjar hundratals datorer samtidigt för att bombardera det tänkta målet. Vanligtvis känner inte ägaren till att deras dator används för att utföra en DDoS-attack. Detta beror på att angriparen har installerat ett dolt program i de angripnas datorer som startar vid ett specifikt klockslag, en viss dag. Installationen av detta program kan angriparen göra dolt genom att t ex skicka ett E-postbrev vilket i sin tur innehåller ett virus (Trojan) som har DDoS-funktionalitet.

1.2.2 Falsk signalering

Falsk signalering som av oss uppfattas som äkta kan leda till intrång i våra telekommunikations- och IT-system. Falsk signalering kan även komma att nyttjas för att överbelasta våra telekommunikations- och IT-system (se DoS-attack i föregående avsnitt). Falsk signalering mot datorer är en typ av datorintrång (”hacking”).

För att bedriva falsk signalering krävs ofta noggranna förberedelser. Underlag kan inhämtas genom signalunderrättelsetjänst. Mot enheter som använder offentliga abonnentnummer såsom telefon- och faxnummer samt IP-adresser, kan falsk signalering utföras utan omfattande förberedelser.

1.3 Exempel på hot

Vi måste förutsätta att all vår telekommunikation kan vara utsatt för avlyssning och påverkan. Detta gäller särskilt den trafik som förmedlas utanför vårt lands gränser. I vissa fall kan även trafik mellan två abonnenter i Sverige ske via utlandet utan abonnenternas vetskap.

1.3.1 Avlyssning

Telefoni och telefax

För användaren är förmodligen avlyssning den mest uppenbara formen av telehot. Avlyssning av våra telelinjer kan ske dels genom inkoppling, t ex i telestation eller teleskåp och dels genom avlyssning med särskild mottagarutrustning av den teletrafik som överförs med radiosändning (radiolänk) och satellit.

Fax med inprogrammerad egen identitet, oftast namn eller faxnummer, sänder denna information i klartext, vilket innebär att faxens identitet kan uppfattas av obehörig. Observera att detta även gäller kryptofax.

TETRA

TETRA (Terrestrial Trunked Radio) är ett radiobaserat kommunikationssystem som, för användning inom räddningstjänst, polis m m, sänder i frekvensområdet 380–395 MHz. I Sverige kallas detta system RAKEL, utbyggnaden av detta system beräknas vara avslutad under år 2010.

Systemet har likheter med GSM där kommunikationen går via basstationer men kan också kommunicera direkt mellan olika terminaler (handhållna & fordonsmonterade radiostationer). En annan sak som också skiljer TETRA från GSM är att en terminal kan kommunicera med flera andra terminaler samtidigt.

Det logiska skyddet i TETRA består av kryptering på länknivå, dvs kryptering sker i luftgränssnittet mellan terminal och basstation och mellan terminal och terminal, i de fall de kommunicerar direkt med varandra utan att gå via en basstation. Kommunikationen går i klartext på alla ställen som inte går i luften.

Krypteringen i Tetra är *inte* godkänd för att skydda hemliga uppgifter.

Data

I takt med ökad nätverks- och Internetanvändning kommer avlyssning av datakommunikation att bli allt vanligare.

I lokala nätverk (LAN) kan avlyssningen ske genom att ansluta en persondator som innehåller en särskild programvara, sk ”sniffer”, till nätverket. Denna typ av programvara kan hämtas gratis på Internet.

Avlyssning av trådlösa nätverk (Radio LAN/WLAN) kan göras med hjälp av särskild programvara som finns lätt tillgänglig på Internet. Sådan avlyssning kallas populärt för ”War driving”. Avlyssningsavståndet ligger normalt på några hundra meter men kan ökas avsevärt (flertalet kilometer) om särskilda antenner och mottagare används.

Idag finns olika standarder för kryptering av WLAN men inga av dessa är godkända för att skydda hemliga uppgifter.

Mobiltelefoni

GSM och UMTS (i dagligt tal kallat 3G) är digitala mobilkommunikationssystem som är något svårare att avlyssna eftersom radiosändningen mellan telefon/terminal och basstation i allmänhet är krypterad. För GSM används frekvensområden på 900 och 1800 MHz och för UMTS används 2300 MHz. Det bör dock påpekas att trafiken i det fasta nätet förmedlas i klartext. Krypteringen i dessa system är *inte* godkända för att skydda hemliga uppgifter.

En metod att avlyssna mobiltelefoni är att använda sig av *falska basstationer*. Genom att upprätta en sådan basstation i närheten av den mobiltelefon som avses avlyssnas kan telefonen ”luras” att ansluta till den falska basstationen.

När GSM-trafik går genom den falska basstationen dekrypteras trafiken och kan avlyssnas av obehörig. Basstationen måste givetvis anslutas till det ”riktiga” GSM-nätet för att denna typ av attack skall kunna genomföras.

Telefoni via sladdlösa telefoner

Analoga system saknar avlyssningsskydd för radiosändningen mellan telefonlur och telefonapparat. Systemen nyttjar ett begränsat antal kanaler och är därmed mycket lätta att avlyssna.

DECT som är ett digitalt system är något svårare att avlyssna eftersom radioförbindelsen mellan telefon och radioterminal är krypterad, det bör dock påpekas att DECT-trafiken i det fasta nätet förmedlas i klartext. Även här gäller det att krypteringen *inte* är godkänd för att skydda hemliga uppgifter.

Personsökningssystem

MINICALL är ett system för mottagning av telefonnummer och/eller textmeddelanden i klartext. Systemet är uppbyggt på särskilda sändare som täcker stora delar av landet. Eftersom systemet inte håller reda på var en viss personsökare befinner sig, sänds alla meddelanden ut över samtliga sändare i landet. Detta möjliggör avlyssning av samt-

liga meddelanden som sänds, oavsett var i landet avlyssningen sker. Vissa larmsystem använder MINICALL för att förmedla statusinformation. Genom att avlyssna MINICALL-meddelande kan obehörig få tips om utslagna larm eller bekräftelse på en informationsoperation mot ett larmsystem.

1.3.2 Påverkan

Instruktioner och order som skickas via tele- och datakommunikation kan spelas in av obehörig för att vid ett senare tillfälle spelas upp i syfte att exempelvis skapa förvirring eller för att få tillgång till information.

En avsändares IP-adress och e-postadress kan enkelt förändras så att mottagaren av exempelvis ett e-postbrev tror att det kommer från en legitim avsändare.

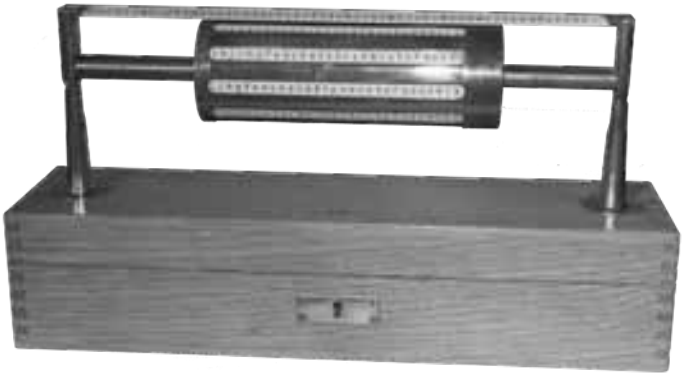
Påverkan och därmed obehörig insyn kan ske genom att ett dolt program (skadlig kod) som har till uppgift att vidareförmedla lagrad information till obehörig, inplanteras i klienter och servrar t ex via bifogade filer i E-post.

Datasystem som inte använder stark autentisering vid inloggning kan utsättas för intrång genom att angriparen relativt enkelt kan gissa rätt användarnamn och lösenord. För ändamålet finns det dessutom särskilda datorprogram att hämta från Internet, vilka kan hjälpa en obehörig att testa igenom möjliga lösenord.

Påverkan genom falsk signalering med fax kan ske genom att avsändaren programmerar in falsk identitet. På detta sätt kan falska meddelanden tas för äkta.

KAPITEL 2

Signalskyddsmetoder



Signalskyddets syfte är att med hjälp av kryptografiska metoder och övriga signalskyddsåtgärder såsom skydd mot signalspaning, störsändning och falsk signalering förhindra obehörig insyn i och påverkan av våra telekommunikations- och IT-system.

Genom att nyttja signalskydd i våra telekommunikations- och IT-system förhindras alternativt försvåras för obehöriga att

- få tillgång till, tyda eller förvanska uppgifter som kommuniceras eller lagras
- påverka våra telekommunikations- och IT-system
- lokalisera varifrån kommunikation sker.

De vanligaste signalskyddsåtgärderna är kryptering, täckning, omskrivning, radiotystnad, bandspridning, val av kommunikationsmedel, användning av digitala signaturer för säker verifiering av elektroniska dokument samt stark autentisering för skydd mot intrång.

För att signalskyddsåtgärder i dagens komplexa system skall ge avsedd skyddseffekt måste de oftast kompletteras med övriga IT-säkerhetsåtgärder.

Signalskyddet anpassas till

- hotet i form av risk för obehörig insyn i och påverkan av telekommunikations- och IT-system,
- kraven på informationsöverföring (tid, mängd m m) samt
- kraven på sekretess vid överföring och lagring av uppgifter.

Ett effektivt signalskydd skapas genom att materiel för signalskyddssystem och system för överföring, bearbetning och lagring av information anpassas till varandra. Detta genom att metoder, regler och instruktioner utformas korrekt och pedagogiskt samt att rätt utbildad personal handhar systemen.

Signalskyddet säkerställs genom

- utveckling, anskaffning och användning av godkända signalskyddssystem,
- samordnad ledning och planering,
- gemensamma föreskrifter, allmänna råd och systeminstruktioner,
- samordnad utveckling och anskaffning av signalskyddsmateriel,
- samordnad produktion och distribution av kryptonycklar, mjuka certifikat samt aktiva kort,
- samordnad utbildning,
- uppföljning i form av administrativa kontroller och signalkontroll.

Signalskyddet vidmakthålls genom att

- kryptonycklar och aktiva kort skyddas mot obehörig insyn och påverkan,
- kryptonycklar byts, förstörs eller raderas enligt gällande rutiner,
- signalskyddsincidenter snarast åtgärdas, exempelvis genom att en kryptonyckel som antas vara röjd ersätts,

- manipulation av signalskyddsmaterielen förhindras,
- instruktioner för signalskyddssystemen efterlevs,
- kvaliteten på signalskyddsmateriel och signalskyddsmetoder fortlöpande följs upp,
- signalskyddstjänsten kontrolleras och följs upp,
- felaktigheter vid handhavandet av signalskyddssystem analyseras och åtgärdas,
- erforderlig utbildning genomförs,
- kunskapen vidmakthålls genom regelbunden användning av signalskyddssystemen samt genom deltagande i repetitionsutbildning och övningar.

2.1 Signalskyddsgrader

Varje signalskyddssystem avsett för sekretesskydd är godkänt upp till och med en viss signalskyddsgrad (SG). Signalskyddsgrad är således ett mått på signalskyddssystemets maximala styrka.

Signalskyddsgrad används även för märkning av kryptonycklar. Märkningen anger vilken signalskyddsgrad en viss nyckelserie är godkänd för samt ger vägledning för nyckelns hantering.

Ett signalskyddssystem som är avsett för skydd av uppgifter som omfattas av sekretess enligt sekretesslagen (1980:100) skall i samband med Högkvarterets godkännande placeras i någon av nedan angivna signalskyddsgrader med följande beteckningar och betydelser.

4 § FFS 2005:2

De signalskyddsgrader som används är:

Tabell 1. Signalskyddsgrader

Signalskyddsgrad	Betydelse
SG TS	Signalskyddssystemet är godkänt för att behandla information som är kvalificerat hemlig, hänförs till informationssäkerhetsklassen HEMLIG/TOP SECRET, internationellt är klassad TOP SECRET eller om den röjs skulle förorsaka totalförsvaret eller förhållandet till annat land eller mellanfolklig organisation synnerligt men.
SG S	Signalskyddssystemet är godkänt för att behandla information som är hemlig, men inte kvalificerat hemlig, hänförs till informationssäkerhetsklassen HEMLIG/SECRET, internationellt är klassad SECRET, eller om den röjs skulle förorsaka totalförsvaret eller förhållandet till annat land eller mellanfolklig organisation betydande, men inte synnerligt, men.
SG C	Signalskyddssystemet är godkänt för att behandla information som hänförs till informationssäkerhetsklassen HEMLIG/CONFIDENTIAL, internationellt är klassad CONFIDENTIAL, eller om den röjs skulle förorsaka totalförsvaret eller förhållandet till annat land eller mellanfolklig organisation inte obetydligt, men inte betydande eller synnerligt, men.
SG R	Signalskyddssystemet är godkänt för att behandla information som hänförs till informationssäkerhetsklassen HEMLIG/RESTRICTED, internationellt är klassad RESTRICTED, eller om den röjs skulle förorsaka totalförsvaret eller förhållandet till annat land eller mellanfolklig organisation endast ringa men.
	4 § FFS 2005:2

Signalskyddssystemets faktiska styrka vid nyttjandet avgörs dels av signalskyddssystemets maximala styrka, dels av kryptonyckelns märk-

ning. Den faktiska signalskyddsgraden är den lägsta av signalskyddssystemets maximala styrka och kryptonyckelns märkning. För exempel, se tabell 2.

Tabell 2. Exempel på faktisk signalskyddsgrad

Signalskyddssystemets maximala styrka	Kryptonyckelns märkning	Faktisk signalskyddsgrad
SG C	SG S	SG C
SG S	SG S	SG S
SG S	SG R	SG R

Ett signalskyddssystem som är godkänt för en viss signalskyddsgrad kan, under förutsättning att informationen har underrättelsevärde under en kort tid (t ex taktisk information), även användas för att skydda information som kräver en högre signalskyddsgrad. Detta framgår i så fall av signalskyddssystemets godkännandeskrivelse och driftsättningsskrivelse.

2.2 Kryptografiska metoder

Symmetriska krypton

Krypto syftar till att hindra obehörig att tyda överförd eller lagrad information under den tid den behöver döljas. Detta åstadkoms genom att informationen, den s k klartexten, med hjälp av en kryptoalgoritm och kryptonyckel omvandlas till kryptotext. För att kunna tolka kryptotexten behövs en likadan kryptonyckel och kryptoalgoritm. Denna typ av krypto kallas symmetriskt.

Beroende bland annat på informationens format används ström- eller blockkrypto.

Om de data som skall krypteras har godtycklig längd är det ofta lämpligast att kryptera bit för bit vartefter de stoppas in i kryptoalgoritmen. Detta kallas strömkrypto.

Om de data som skall krypteras är uppdelade i block av lika längd kan det passa bättre att kryptera block för block, t ex 128 bitar i taget. Detta kallas blockkrypto.

Symmetriska krypton ger i första hand skydd mot insyn (sekretesskydd). Finns starka krav även på att kunna upptäcka ändring av data måste ytterligare någon skyddsmekanism användas, t ex ett blockkrypto i kombination med någon form av checksumma.

Asymmetriska krypton

På 1970-talet utvecklades idéer om krypton med olika nycklar för kryptering och dekryptering. Detta innebär att varje användare har ett sammanhörande par av nycklar, en privat och en publik.

Om ett meddelande skall krypteras använder avsändaren mottagarens publika nyckel för att kryptera meddelandet och mottagaren dekrypterar det med sin privata nyckel.

Om man istället vill autentisera sig eller signera ett meddelande (för att erhålla riktighet och oavvislighet), använder avsändaren sin privata nyckel till att signera information på ett sätt som binder innehållet till användaren och även gör det möjligt att upptäcka eventuella förändringar av informationen efter det att den signerats. Den publika nyckeln sprids till alla de som behöver verifiera avsändare och korrekthet hos mottagen information.

Vanligen används ett specifikt nyckelpar för autentisering och kryptering och ett annat för signering (digital signatur).

Säkerheten i systemet bygger på att även med kännedom om den ena nyckeln i paret är det en mycket arbetskrävande uppgift att beräkna den andra. Den privata nyckeln måste naturligtvis förvaras så att ingen annan än den behörige användaren kan komma åt den.

Ett exempel på asymmetriskt krypto är RSA som är uppkallad efter sina konstruktörer Rivest, Shamir och Adleman.

För att en mottagare skall kunna lita på att en publik nyckel hör till en avsändare sprids den i form av ett certifikat. Certifikatet är ett signerat

intyg från CA (Certification Authority) att en publik nyckel hör till en viss avsändare. Systemet bygger på tilltro till CA och därmed även tilltro till de certifikat som CA signerat. Första steget i kedjan måste alltid vara att användaren har tillgång till och kan lita på CA: s publika nyckel för att kunna verifiera mottagna certifikat.

Om en användare har förlorat sin privata nyckel och certifikatet därmed ej längre är giltigt, tillkännages detta i en så kallad revokeringslista (CRL) som utges av CA.

Vissa aktiva kort (TAK och TEID) har användarens privata nycklar lagrade så att de inte kan läsas ut ur kortet utan endast användas efter angivande av PIN. TAK och TEID levereras med CA:s publika nyckel inläst på korten så att användaren kan verifiera mottagna meddelanden. TAK och TEID innehåller även användarens certifikat som kan bifogas signerade meddelanden.

Hashsummor

En hashfunktion avbildar ett meddelande av godtycklig storlek på en datasträng med fast längd, vanligen 160 eller 256 bitar. Denna sträng kallas hashsumma, checksumma eller kondensat.

En hashsumma har flera viktiga egenskaper.

- Den är lätt att beräkna.
- Det skall vara svårt att beräkna meddelandet även om man känner till hashsumman.
- En ändring av meddelandet skall medföra en ändring av hashsumman.
- Det skall vara beräkningsmässigt svårt att hitta två olika meddelanden som ger samma hashsumma.

Hashsummor beräknas med kända algoritmer och måste signeras eller krypteras för att undvika obehörig förändring.

2.2.1 Användningsområden

Kryptografiska metoder kan bl a användas för:

- sekretesskydd av information,
- kontroll av uppgiven identitet,
- kontroll av ett meddelandes riktighet samt
- att ge intrångsskydd för datorer eller nätverk.

Sekretesskydd

Ett signalskyddssystem får i regel användas för att skydda information med högst den signalskyddsgrad som anges i den godkännandeskrivelse som reglerar hantering eller användning av systemet. Signalskyddsgrad är ett mått på det sekretesskydd som signalskyddssystemet kan ge. För sekretesskydd används normalt symmetriska krypton.

Identitet

Asymmetriska krypton ger möjlighet att binda ett signerat dokument till den som signerat samt styrka en användares identitet vid inloggning.

Riktighet

För att kunna upptäcka ändring av informationen vid överföring eller lagring beräknas en hashsumma som, signerad eller krypterad, bifogas informationen.

Skydd mot intrång

För att en kryptofunktion eller kryptoutrustning skall kunna skydda mot intrång via ett nät krävs att den är placerad mellan det som skall skyddas och nätet samt att det har verifierats att all kommunikation passerar på korrekt sätt genom kryptot.

2.2.2 Krav för godkännande

För att godkänna användning av en kryptografisk funktion krävs

- godkänd implementation av en godkänd algoritm samt
- godkänd nyckelhantering.

Dessutom krävs för varje användningsmiljö en särskild bedömning om att eventuella krav på riktighet, identifiering och intrångsskydd är uppfyllda.

2.3 Kryptering och dekryptering

Kryptering kan utföras för hand (handkrypto), med ett program (programvarukrypto) eller med hjälp av krypteringsapparat (maskinkrypto). Maskinkrypto används även som beteckning på en i dator integrerad krypteringsfunktion (t ex kryptokort).

Oavsett klartextens ursprungliga form, t ex skrift, data, bild eller tal, digitaliseras informationen för att kunna krypteras med ett maskinkrypto.

Handkrypto används företrädesvis vid enheter med begränsat sambandsbehov och vid överföring av uppgifter, som endast skall delges en mycket begränsad krets av personer. Idag finns endast Handchiffer Gemensamt typ E (HGE).

För att få ett fullgott signalskydd nyttjas totalsträckskryptering (end-to-end encryption), varvid informationen överförs krypterad hela sträckan från avsändare till mottagare.

Vid delsträckskryptering omkrypteras informationen efter varje delsträcka. Detta medför att både kryptonycklar och klartext förekommer i varje knutpunkt i ett nät.

Om mottaget meddelande inte kan dekrypteras underrättas avsändaren med ett kryptotjänstmeddelande. Meddelandet åsätts SG S.

Fel som bedöms kunna äventyra ett systems säkerhet måste omedelbart anmälas till Högkvarteret (TSA). Att inte anmäla upptäckta fel kan medföra allvarliga konsekvenser för rikets säkerhet.

Om krypterings- eller dekrypteringsarbete utförs i dator bör det säkerställas att lagrad klartext inte blir åtkomlig för obehörig. Arbetspapper som har använts vid krypterings- och dekrypteringsarbete förstörs snarast efter det att arbetet har avslutats.

Engångskod

Engångskod är ett system för kryptering av order angående viss planlagd verksamhet eller för rapportering av viss förutsedd händelse eller åtgärd. Kryptering och dekryptering utförs med hjälp av *kodord som används endast en gång i samma betydelse*. Engångskod kan användas för meddelanden av samtliga signalskyddsgrader. Den som beordrar att engångskod skall användas är även ansvarig för lottning av kodord.

I en krypterad text kan ingå ett eller flera kodord. Skriftlig krypterad text inleds alltid med den fasta gruppen *KODOR*. Kryptobeteckning används inte i ett kodordsmeddelande. I personsamtal ersätts *KODOR* t ex med *"Jag använder engångskod"*. Använda kodord stryks efter hand i förteckningens sändnings- och mottagningsdel. Om meddelande med kodord repeteras skall samma kodord användas.

Kodord utgörs av en femställig bokstavsgrupp där andra och fjärde bokstaven utgörs av en vokal. Ordet måste vara uttalbart.

Tabell 3. Exempel på engångskod för viss verksamhet

A. Avsändningsdel		*B. Mottagningsdel*	
Klartext	**Kodord**	**Kodord**	**Klartext**
Radiotystnad upphör	JUMIF	BELOX	Använd reservfrekvens
	LIVAT	~~FASON~~	Radiotystnad upphör
	~~FASON~~	JUMIF	Radiotystnad upphör
Använd reservfrekvens	KUREM	KUREM	Använd reservfrekvens
	BELOX	LIVAT	Radiotystnad upphör
Återkalla permitterade	~~MOKOT~~	~~MOKOT~~	Återkalla permitterade

~~FASON~~ = Kodordet har använts.

Anvisningar för användande av engångskod framgår även av instruktion i blankettblock "*ENGÅNGSKOD*" (M7102-122490).

2.4 Täckning

Till system för täckning räknas täcktabeller, tillfälliga lägesangivningssystem och tillfälliga verksamhetstabeller. Vid täckning omvandlas klartext till blandad text. Dessa system är som regel godkända för signalskyddsgrad SG R.

Tillfälliga lägesangivningssystem och tillfälliga verksamhetstabeller används vid taktisk verksamhet för att under begränsad tid snabbt och kortfattat dölja innehållet i order och rapporter.

Vid behov upprättar chef tillfälligt lägesangivningssystem och tillfällig verksamhetstabell för användning inom eget ansvarsområde.

Den som avser att nyttja täcksystem skall förvissa sig om att mottagaren har möjlighet att tolka texten.

Råkar någon försäga sig genom att använda klartextuttryck i stället för en täckterm, får felsägningen inte påpekas eller rättas.

Uppgift om att ett täckt meddelande inte kan tolkas får normalt sändas i klartext.

Täcktabeller

Med hjälp av täcktabell och tillhörande täcknyckel ersätts vissa ord, uttryck eller enskilda tecken i klartexten med täcktermer.

Klartext redigeras så att täcktabellens ord och uttryck kan nyttjas för att skydda innebörden i texten. Sedan väsentliga uppgifter har täckts får kvarvarande klartext inte röja täcktermernas betydelse.

Ord täcks bokstav för bokstav endast om klartextdelen i tabellen innehåller bokstäver som är avsedda för bokstavering.

Innehåller täcktabell mer än en täckterm för samma uttryck används dessa omväxlande. Om det bara finns en täckterm för ett visst uttryck varieras denna om möjligt med täckterm för andra ord eller uttryck som har motsvarande innebörd.

Täcktabell försedd med täcknyckel eller kompletteringstabell hanteras som hemlig handling, detta gäller även blankett som innehåller såväl klartext som motsvarande täckterm.

Tillfälliga lägesangivningssystem

Tillfälliga lägesangivningssystem kan användas för att under begränsad tid eller för ett bestämt tillfälle dölja uppgift om geografiskt läge. Läge anges i det sammanhanget med koordinater i tillfälligt rutnät eller genom hänvisning till en på förhand överenskommen punkt. Klartextbenämningar får inte blandas med uppgift ur tillfälligt lägesangivningssystem.

Om motståndarens geografiska läge anges med hjälp av samma tillfälliga lägesangivningssystem som används för att ange egna förbands läge, äventyras säkerheten i lägesangivningssystemet.

Används tillfälliga lägesangivningssystem gäller underlaget med vars hjälp läge anges, endast så länge viss verksamhet pågår. Underlaget kan ändras genom att dess läge på kartan varieras.

Tillfälliga verksamhetstabeller

Tillfällig verksamhetstabell – TIVETA – används för att täcka texten till meddelanden av signalskyddsgrad SG R. Tabellen bör gälla avgränsat taktiskt uppdrag, dock högst två dygn. Nyckeln består av tabeller med plats för 25 eller 50 olika klartextuttryck. Endast fyrställiga täcktermer utnyttjas. Anvisningar för användande av tillfällig verksamhetstabell framgår av instruktion i blankettblock *"TIVETA"* (M7102-122480).

2.5 Omskrivning

Vid omskrivning omvandlas klartext till blandad text. Omskrivning ger inte något väsentligt signalskydd om hänvisning sker till handlingar, händelser eller sakförhållanden som kan anses vara allmänt kända.

Omskrivning kan ge ett bra signalskydd om hänvisningshandling är hemlig, har begränsad spridning och endast används för omskrivning vid ett fåtal tillfällen.

Hänvisning till handling kan till exempel avse sida, rad och kolumn. Standardblankett får dock inte användas som hänvisningshandling. Alternativt kan hänvisning göras till händelse eller sakförhållande som inte är kända för utomstående. Omskrivning bör användas restriktivt.

2.6 Trafikskydd

Signalskydd i form av trafikskydd omfattar skydd mot signalunderrättelsetjänst, skydd mot störsändning och skydd mot falsk signalering (kommunikation). Detta uppnås genom

- utbildning i och information om hot mot telekommunikations- och IT-system,
- användning av trafikskyddsmetoder och trafikskyddsmateriel i telekommunikations- och IT-system,
- rätt utformad taktik för kommunikationen,
- iakttagande av regler och instruktioner för kommunikationen.

Trafikskyddets syfte är att

- hindra eller försvåra för obehörig att upptäcka, avlyssna, pejla samt positionera våra telekommunikations- och IT-system,
- hindra eller försvåra trafikanalys,
- minska verkan av störsändning,
- hindra eller minska verkan av falsk kommunikation t ex datorintrång,
- möjliggöra upptäckt av obehörig ändring eller manipulation av kommunicerad eller lagrad information.

2.6.1 Skydd mot signalunderrättelsetjänst

Skydd mot signalunderrättelsetjänst åstadkoms bl a genom

- val av medel för kommunikation,
- radiotystnad,
- val av grupperingsplats för radiofrekvent strålande materiel,
- materielutformning,
- användning av kryptografiska metoder,
- snabb och likformig trafikavveckling,
- användning av rörliga anropssignaler och frekvenser samt
- fyllnadssignalering och maskerande signalering.

Val av metod för kommunikation

Ur trafikskyddssynpunkt väljs kabel (optofiber och tråd) samt optiska eller hydroakustiska medel före radio eller radiolänk.

Tråd- och optofiberförbindelser bör anordnas på sådant sätt att obehörig inkoppling försvåras eller omedelbart kan upptäckas. Obehörig fysisk inkoppling försvåras genom att tillträdesskydd och speciella säkerhetsåtgärder vidtas. Sådana åtgärder kan vara bevakning eller larmning av särskilt viktiga och lättåtkomliga kablar och kopplingspunkter.

Vid optisk signalering, t ex infraröd, vidtas åtgärder för att begränsa strålningen till aktuell förbindelseriktning och till erforderligt förbindelseavstånd.

Vid radioförbindelse väljs antenn, grupperingsplats, frekvensområde och sändareffekt med hänsyn till aktuellt telehot och rådande vågutbredningsförhållanden. Allmänt gäller att mikrovågsförbindelser är mera svåråtkomliga för signalspaning än ultrakortvågsförbindelser, och att de senare är mera svåråtkomliga än kortvågs- och långvågsförbindelser.

Vid all kommunikation beaktas risken att röjande bakgrundsinformation, t ex samtal, kommer ut på förbindelsen.

För att försvåra motståndarens signalspaning kompletteras val av kommunikationsmetod med tekniska åtgärder såsom

- snabbsändning,
- bandspridning genom frekvenshopp eller direktsekvens,
- effektanpassning,
- nyttjande av antenn med riktverkan samt
- kryptering.

Radiotystnad

Radiotystnad syftar till att

- hindra främmande signalunderrättelsetjänst att få upplysningar om vår pågående och planerade verksamhet,

- försvåra lokalisering av våra anläggningar och enheter,
- minska underlaget för främmande signalunderrättelsetjänsts bearbetning av vår telekommunikation.

Chef kan besluta om radiotystnad för egen och underställda enheter samt även för de enheter som lyder under honom beträffande sambandstjänst.

Radiotystnad kan beordras för

- frekvensområden och frekvenser,
- trafiknät,
- geografiskt område,
- enhet eller verksamhet samt för
- bestämd tid.

Radio- och radartystnad bör samordnas så långt detta är möjligt. På samma sätt samordnas radio- och radartystnad med förbud mot användning av annan elektromagnetiskt strålande utrustning i ultrakortvågs- och mikrovågsbanden.

Radiotystnad får inte tillämpas stereotypt. Om den t ex alltid tillämpas i samband med operationer av visst slag kommer den att kunna röja dessa för motståndaren.

Vid avsteg från anbefalld radiotystnad underrättas den chef som beordrat radiotystnaden om möjligt på annat sambandsmedel än radio. Att en enhet i eget nät brutit radiotystnad innebär inte att andra enheter därmed får bryta radiotystnaden.

Gruppering av radiosändare

Sändarplats väljs så att motståndaren ges begränsad möjlighet att lokalisera stabsplatsen genom sin kännedom om terrängens möjligheter och om våra grupperingsprinciper. Sändarplats bör därför grupperas i olika riktningar och på varierande avstånd i förhållande till stabsplats.

Strålning från radiosändare i riktning mot motståndaren bör begränsas.

Vågutbredning beaktas genom att nyttja

- radioskugga vid val av sändarplats,
- antennernas riktverkan,
- lägsta användbara sändareffekt.

Utformning och tilldelning av materiel

Användande av kommunikationsutrustningar med individuella sändaregenheter medför att en enhet kan identifieras. Vid utformning av materiel beaktas att en radiosändare inte får avge en unik signalbild. Vid teknisk kontroll och materielunderhåll bör eventuella egenheter korrigeras.

Vid tilldelning av materiel beaktas att enheter kan bli identifierade om de använder kommunikationsutrustning som har allmänt kända eller unika egenskaper och förekommer endast i enstaka exemplar.

Kryptering

Kryptering kan användas för att skydda telekommunikation mot trafikanalys. Genom att ständigt kryptera varje delsträcka i ett radiolänknät oavsett om det går trafik i nätet eller inte, kan en obehörig ej utläsa kommunikationens volym, vägar, intensitet, metoder samt förekomst av krypto- och klartexter.

Ett signalskyddssystem som i huvudsak används för skydd av hemliga uppgifter ger även ett visst trafikskydd. Ett exempel på detta är användning av VPN-krypto (virtuellt privat nätverk). Detta ger en säker och skyddad kommunikation mellan två eller flera lokala nätverk (LAN) som använder publika nät för kommunikation mellan sig.

När VPN-krypto används mellan lokala nätverk krypteras både adresser och information. För att det publika nätverket skall kunna skicka (”routa”) datatrafiken till rätt mottagare måste dock datatrafiken innehålla avsändar- och mottagaradress (IP-adresser) i klartext. Krypteringsapparaten löser detta genom att, i datatrafiken, lägga till sin egen samt mottagande kryptoapparats IP-adress i klartext. Mottagande

krypto dekrypterar den inkommande datatrafiken, utläser adressen till den rätta mottagaren i det lokala nätverket och skickar därefter den vidare till rätt slutdestination.

Obehörig som lyssnar på VPN-krypterad kommunikation mellan två nätverk kommer att upptäcka att det går trafik mellan dem, men kan t ex inte utläsa hur många datorer som finns på respektive nätverk då deras adresser alltid är krypterade.

Trafikavveckling vid radiokommunikation

Snabb trafikavveckling och lämpligt val av trafikmetod försvårar upptäckt och avlyssning av vår telekommunikation samt positionering av våra sändare.

Snabb trafikavveckling åstadkoms genom att

- kommunikationen utförs av utbildad personal,
- endast nödvändig kommunikation utförs,
- god passning sker,
- omfrågning och repetition undviks,
- meddelanden formuleras kort och med fastställda ord och uttryck.

Snabbsändning ger ett visst skydd mot upptäckt och pejling. Detta kan ytterligare förstärkas genom att använda rörliga frekvenser samt sända på oregelbundna tider.

Enkelriktad signalering är en trafikmetod som kan användas för kommunikation till enheter som behöver skyddas mot upptäckt eller mot positionering.

Vid dubbelriktad kommunikation kan visst skydd mot positionering och trafikanalys erhållas om en av enheterna inom ett förband eller motsvarande avdelas för all kommunikation med andra förband.

Provsändning och nätjustering

I fred får sändning med radio och radiolänk från anläggningar i sekretessklass 1 och 2 endast ske efter tillstånd av Högkvarteret.

Förbindelse provas

- endast i den utsträckning det är nödvändigt för förbindelsens funktion,
- kortast möjliga tid vid sändning över öppen antenn,
- utan anropssignaler eller andra adressuppgifter,
- genom korta förbindelseprov om möjligt ledda över kabel,
- med maskinellt framställd provtext samt
- med lägsta användbara effekt.

Förbindelseprov vid rörliga enheter utförs på sådant sätt och vid sådan tid att provet icke röjer kommande verksamhet.

Meddelande om planering, genomförande, rapportering och övriga omständigheter som berör en provsändning åsätts lägst SG S.

Anropssignaler

Anropssignaler används bl a för att underlätta signalering. Anropssignalerna indelas i rörliga, fasta och tillfälliga.

En form av anropssignaler är IP-adresser som används vid datakommunikation. Dessa adresser tilldelas globalt och utgör unika teleadresser inom ett nätverk.

Rörliga anropssignaler på radio används för att försvåra identifiering och bör användas av enhet som kräver identitetsskydd. För att förstärka identitetsskyddet bör byte av anropssignal, frekvens och signalist ske samtidigt.

Fasta anropssignaler som används för att underlätta signalering, ger inget eller mycket lågt identitetsskydd.

Tillfälliga anropssignaler tilldelas enheter för att ge ett bättre identitetsskydd och bör användas vid

- särskilda uppdrag,
- hemliga prov och försök samt vid
- upprättande av samband efter en omgruppering som utförts under radiotystnad.

Gemensam eller geografisk anropssignal används om möjligt för krypterade meddelanden vid enkelriktad signalering. Alla enheter som omfattas av den gemensamma anropssignalen eller befinner sig i samma geografiska område tar emot och dekrypterar meddelandet. Vid användning av gemensam eller geografisk anropssignal inkrypteras adressuppgifter i meddelandet.

För att hindra att identitetsskyddande anropssignaler röjs

- slutförs pågående kommunikation med den ursprungliga anropssignalen och radiofrekvensen,
- slutförs pågående kommunikation även om felaktig anropssignal har använts,
- krypteras hänvisningar till tidigare löpnummerserie,
- krypteras ett meddelande som berör förhållanden som anropssignaler skall dölja.

Frekvenser

Inom Försvarsmakten regleras frekvensanvändning i Försvarsmaktens handbok för frekvensplanering (H FM Frekvens). För civila myndigheter regleras detta av Post- och Telestyrelsen (PTS).

Rörlig frekvens tillsammans med rörlig anropssignal kan av taktiska skäl användas för att försvåra identifiering. Frekvens och anropssignal bör bytas samtidigt.

Fasta frekvenser byts vanligen endast av trafikala skäl, t ex till rådande vågutbredningsförhållanden. Nya frekvenser nyttjas för att tillfälligt försvåra upptäckt.

Frekvensövergång i trafikskyddande syfte bör beordras med kodord. Frekvensangivelse kan skyddas med särskild beteckning.

Fyllnadssignalering och maskerande signalering

Fyllnadssignalering och maskerande signalering benämns vilseledande signalering.

Radiostation, som utför vilseledande signalering, kan pejlas. Denna risk vägs mot de fördelar som signaleringen väntas ge.

Maskerande signalering utförs för att försvåra upptäckt av viss sändning, främst vid provsändning från hemlig anläggning och vid prov och försök.

För att dölja förändringar i det operativa eller taktiska läget används fyllnadssignalering. Den utförs i ordinarie trafiknät för att åstadkomma ett jämnt fördelat trafikflöde eller oregelbundna återkommande trafiktoppar för att skapa en ”falsk normalbild”.

Fyllnadssignalering får inte skilja sig från ordinarie trafik. Signaleringen måste utföras på ett verklighetstroget sätt, med samma noggrannhet som ordinarie signalering. Uppgifter rörande planerad, pågående eller utförd fyllnadssignalering är vanligen sekretessbelagda och får delges endast de som behöver dessa för sin tjänst. Signalist bör inte känna till att fyllnadssignalering pågår i eget nät.

För fyllnadssignalering används antingen krypterade meddelanden som innehåller intetsägande klartext eller datorproducerad kryptomassa. Program för framställning av kryptomassa skall vara godkänt av Högkvarteret (TSA).

Sambandschef utarbetar förslag till order för fyllnadssignalering. Förslaget grundas på sambands- och stridsplan. Ordern kan vara stående eller gälla för visst uppdrag.

Övningssignalering

Övningssignalering utförs i första hand på förbindelser i kabel, helst anordnade som internt nät. Saknas lämplig förbindelse överväger chef om övningen kan förläggas till plats där sådan finns.

Övningssignalering på radio och rörlig radiolänk bör genomföras inom särskilt avdelat område med särskilda frekvenser, anropssignaler och utbildningsanordningar.

2.6.2 Skydd mot störsändning

Skydd mot störsändning åstadkoms genom skydd mot signalunderrättelsetjänst kompletterat med störskyddsåtgärder.

Störskyddsåtgärder omfattar planläggning för och användning av

- störtåliga system,
- alternativa kommunikationssystem,
- alternativa vägar för kommunikationen,
- frekvensbyten samt
- vilseledande signalering.

Störsändning riktad mot egen kommunikation rapporteras till sambandschef.

Planlagda skyddsåtgärder bör övas i fred om kraven på sekretess uppfylls. Regler för användning av störsändare vid utbildning i skydd mot störsändning utfärdas av Högkvarteret.

Medel och metoder

När en motståndare försöker störa ut vår kommunikation kan en eller flera av följande metoder tillämpas.

- Spridning av samma meddelande på flera frekvenser samtidigt.
- Riktantenn nyttjas.
- Repeterstation nyttjas för att förlänga förbindelseavståndet.
- Mobila och bärbara radiostationer eller separat anordnade mottagarantenner grupperas om möjligt så att höjder skärmar strålningen från störsändare.
- Sändarens uteffekt ökas när störsändning sätts in.
- Störsändare lokaliseras och oskadliggörs.

Effektsteg, avsett för störskydd, används restriktivt så att den tillgängliga effektreserven inte röjs i förtid.

För att minska verkan av DoS-attacker, som i viss mån kan jämföras med störsändning, kan nätverkskomponenter konfigureras för detta.

Vilseledande signalering

Vilseledande signalering utförs bl a för att dra till sig störsändning. Sådan signalering kan bestå av verkliga meddelanden eller fyllnadssignalering som sänds parallellt med ordinarie signalering.

På utstörd frekvens utförs vilseledande signalering även efter det att övergång till reservfrekvens skett.

2.6.3 Skydd mot falsk signalering

Skydd mot falsk signalering åstadkoms genom skydd mot signalunderrättelsetjänst, kompletterat med behörighetskontroll samt genom äkthetskontroll av mottagen information.

De som kan komma att utsättas för falsk signalering orienteras om hotet, aktuella skyddsåtgärder samt övas i kontroll av behörighet och informationens äkthet. Kryptering kan användas för att försvåra falsk signalering.

Kommunikation i eget nät bör övervakas för att därigenom medverka till att falsk signalering upptäcks. Falsk signalering rapporteras omgående.

Åtgärder vidtas för att hindra eller försvåra för obehörig att få tillgång till kopplingspunkter som kan användas för falsk signalering.

Behörighetskontroll

Behörighetskontroll utförs som lösensignalering, men kan även utföras genom att

- motringning utförs på annan förbindelse,
- röstidentifiering utförs vid personsamtal där frågor och svar inte har kunnat förutses,
- frågor och svar utväxlas rörande förhållanden som kan förutsättas vara okända för obehöriga,
- meddelanden krypteras.

Behörighetskontroll bör utföras då ett meddelande innehåller

- frågor om hemliga förhållanden,

- uppgifter som kan skada vårt samband,
- order om att radiotystnad skall brytas,
- återkallelse av ett tidigare kvitterat meddelande,
- order eller anvisning som gynnar motståndaren samt
- underrättelser om motståndaren vilka inte stämmer överens med vad som tidigare är känt.

Behörighetskontroll vid datakommunikation kan ske med hjälp av stark autentisering, se avsnitt 2.6.4 ”Autentisering och digital signatur.”

Äkthetskontroll

Äkthetskontroll kan utföras genom att

- äktheten av ett meddelande i pågående kommunikation kontrolleras hos avsändaren genom annan förbindelse,
- meddelandet förses med digital signatur, se avsnitt 2.6.4 ”Digital signatur”,
- meddelandet förses med checksumma och krypteras.

2.6.4 Autentisering och digital signatur

För att använda en asymmetrisk metod såsom RSA för autentisering och digital signatur publiceras den publika nyckeln i ett certifikat. Certifikatet kan publiceras i en katalog som alla har tillgång till eller skickas med meddelandet. Den privata nyckeln måste förvaras så att ingen annan än ägaren kan komma åt den. Bäst skydd fås om den privata nyckeln lagras i en fil i ett aktivt kort, där det inte är möjligt att läsa ut den. Kortet förvaras så att endast ägaren kan komma åt det.

Autentisering

För att få så kallad stark autentisering vid inloggning i en dator måste användaren uppge sin identitet samt ange PIN för att få åtkomst till det aktiva kortet.

Datorn skickar ett slumptal (challenge) som överförs till det aktiva kortet. Processorn på kortet utför nu en RSA-operation på slumptalet med den privata nyckel som är avsedd för autentisering. Resultatet sänds tillbaka till datorn (respons).

Datorn utför RSA-operationen på mottagen respons med den uppgivne användarens publika nyckel och får tillbaka det slumptal som skickats som challenge. Datorn vet nu att användaren har tillgång till rätt kort samt PIN för detta.

På detta sätt får man olika ”lösenord” för varje inloggning (engångslösenord) och enbart den som har tillgång till den privata nyckeln kan ge rätt ”lösenord”.

Digital signatur

Digitala signaturer knyter en användare till det signerade dokumentet på samma sätt som en handskriven signatur utgör bevis att någon skrivit/skapat ett dokument. Den digitala signaturen utgör också en kontrollsumma som upptäcker minsta ändring i dokumentet efter att det har signerats.

För att göra en digital signatur för ett dokument eller datamängd skapas först ett kondensat av dokumentet i en så kallad hashsumma. Hashsumman plus utfyllnad sänds till det aktiva kortet som utför en RSA-operation med den privata nyckel som är avsedd för signering. Resultatet utgör den digitala signaturen.

Eftersom signaturen skapats med den privata nyckeln kan alla som har tillgång till den publika nyckeln kontrollera signaturen och därmed även att dokumentet inte har ändrats sedan signeringen. Kontrollen sker genom att mottagaren beräknar en hashsumma för det mottagna dokumentet. Sedan utför mottagaren en RSA-operation med avsändarens publika nyckel på signaturen. Slutligen jämförs resultaten.

2.7 Val av signalskydd

Som utgångspunkt för val av signalskydd vid kommunikation används

- informationens skyddsbehov (val av signalskyddsgrad),
- aktuell telehotbild,
- klartextens form, t ex tal eller data,
- kravet på snabbhet vid överföringen samt
- tillgängliga sambandsmedel.

Kryptosambandstablå upprättas för att redovisa en enhets möjlighet att med hjälp av signalskyddssystem och nyckelserier åstadkomma signalskyddat samband. För tal-, bild- och datakrypto finns i allmänhet endast ett system tillgängligt. Valet består då av vilken nyckelserie som skall användas.

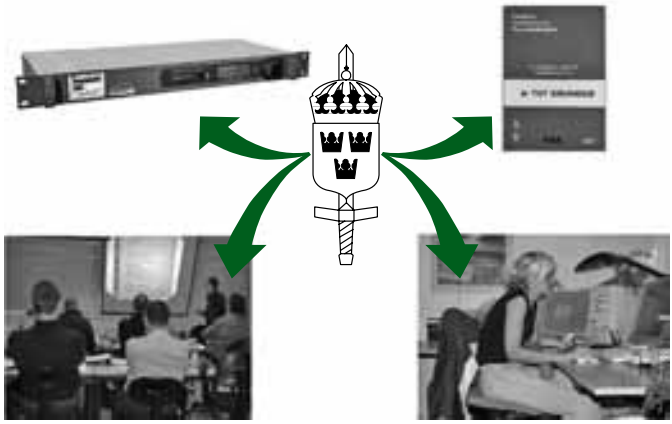
När information skall sändas till flera adressater används i första hand den nyckel ur den nyckelserie som har minst spridning och som *alla* adressater har tillgång till. På detta sätt behöver informationen krypteras endast en gång och samma krypterade information kan sändas till alla mottagare.

Främmande signalunderrättelsetjänst finner ofta värdefulla underrättelser även bland information som inte är sekretessbelagd. Om signalskyddssystem finns tillgängligt bör därför så mycket information som möjligt signalskyddas.

Saknar myndighet eller enhet ett signalskyddssystem som är godkänt för den signalskyddsgrad informationen kräver, skyddas informationen – om den måste överföras via telekommunikation – med starkast möjliga system. Ansvarig chef godkänner och bestyrker att informationen får sändas med detta system.

Myndighet eller enhet som helt saknar egna resurser för signalskydd hänvisas till närmaste myndighet/enhet som har signalskyddsresurser.

KAPITEL 3
Ledning



Av 4 § förordningen (2000:555) med instruktion för Försvarsmakten framgår att Försvarsmakten skall leda och samordna signalskyddstjänsten inklusive arbetet med säkra kryptografiska funktioner inom totalförsvaret. Sådan ledning och samordning utövas av chefen för militära underrättelse- och säkerhetstjänsten i Högkvarteret.

Verkställande organ för denna ledning och samordning är Totalförsvarets signalskyddssamordning (TSA) som är en funktion inom Säkerhetskontoret (SÄKK) vid Militära underrättelse- och säkerhetstjänsten (MUST) i Högkvarteret (HKV).

Varje chef leder och samordnar signalskyddstjänsten inom eget ansvarsområde.

Militära försvaret

Högkvarteret leder och samordnar signalskyddstjänsten inom det militära försvaret.

Civila myndigheter

Krisberedskapsmyndigheten (KBM) samordnar civila myndigheters signalskyddstjänst.

Länsstyrelsen samordnar den regionala signalskyddstjänsten inom respektive län.

Samordning

Företrädare för det militära försvaret och civila myndigheter bör verka för att signalskyddstjänsten samordnas.

3.1 Organisation

Varje myndighet/enhet fastställer sin egen signalskyddsorganisation. En person kan inneha olika signalskyddsbefattningar enligt nedan om verksamheten så kräver, dock skall det säkerställas att signalskyddsorganisationen personellt och materiellt har resurser att bedriva verksamhet i fred, kris och efter höjd beredskap.

Utifrån varje myndighets eller enhets behov utses och utbildas signalskyddspersonal ur följande kategorier.

Signalskyddspersonal

- Signalskyddschef
- Biträdande signalskyddschef
- Systemoperatör
- Kortadministratör
- Nyckeladministratör

Utöver ovanstående signalskyddspersonal kan myndigheten/enheten utse och utbilda nödvändigt antal användare.

Om möjligt bör det dock undvikas att en och samma person innehar samtliga signalskyddsbefattningar vid en myndighet/enhet pga nyckelpersonsberoende och problem med avlastning vid t ex semester, sjukdom eller annan bortavaro.

3.2 Uttagning av personal

Endast den som med godkänt resultat har genomgått erforderlig utbildning i signalskydd får placeras i signalskyddsbefattning eller nyttja, betjäna eller på annat sätt hantera signalskyddsmateriel, kryptonycklar eller aktiva kort.

Varje myndighet skall se till att den personal som inom myndigheten avses få uppgifter som anges i första stycket ges erforderlig utbildning.

10 § FFS 2005:2

Ett särskilt säkerhetsansvar tillkommer den personal som skall placeras i signalskyddsbefattning eller nyttja, betjäna eller på annat sätt hantera signalskyddsmateriel eller kryptonycklar. Sådana befattningar bör på grund av det särskilda säkerhetsansvaret placeras i *lägst säkerhetsklass 3*, enligt vad som framgår av säkerhetsskyddsförordningen. Detta bör uppmärksammas redan vid uttagningen av den aktuella personalen.

Det åligger varje myndighet/enhet att genomföra säkerhetsprövning samt utbildning i säkerhetsskyddstjänst av den personal som skall utbildas i signalskydd, innan personalen påbörjar sin signalskyddsutbildning.

Utbildning i säkerhetsskyddstjänst ges i form av säkerhetsupplysning och säkerhetsutbildning. Utbildning i säkerhetsskyddstjänst sker normalt under ledning av säkerhetschef eller motsvarande. Säkerhetsutbildningen kan t ex omfatta genomgång av säkerhetshotande verksamhet, säkerhetstjänstens uppgifter och organisation, samverkande myndigheter eller företag, relevant lagstiftning, föreskrifter och bestämmelser, myndighetens/enhetens säkerhetsskyddsplanering etc. I samband med säkerhetsutbildningen är det även lämpligt att den utbildade undertecknar ett sekretessbevis.

Personal som tas ut till signalskyddsbefattning bör i första hand rekryteras från myndighetens/enhetens ordinarie personal och kunna verka i avsedd befattning minst fem år efter avslutad utbildning.

Den snabba utvecklingen inom signalskyddstjänstens område, främst vad avser materielen, kräver regelbunden förnyad utbildning. Vid osäkerhet om och när en förnyad utbildning bör genomföras, för att exempelvis upprätthålla en viss befattning, kontaktas Totalförsvarets signalskyddsskola (TSS).

Vid uttagning av personal till signalskyddsbefattning bör kopplingen mellan signalskyddsverksamhet och övrig IT-säkerhetsverksamhet uppmärksammas. Detta för att om möjligt åstadkomma positiva samordnings- och samverkanseffekter.

Varje myndighet som innehar signalskyddssystem skall ha en signalskyddschef. Om myndigheten består av flera enheter gäller detta varje enhet. Signalskyddschefen har till uppgift att ansvara för ledning och samordning av signalskyddstjänsten.

Om det finns särskilda skäl får en signalskyddschef vara signalskyddschef för andra enheter inom myndigheten, eller för en annan myndighet eller en eller flera av dess enheter efter överenskommelse mellan berörda myndigheter.

Det skall finnas en biträdande signalskyddschef vid varje myndighet som inte har en egen signalskyddschef. Om myndigheten består av flera enheter gäller detta varje enhet.

7 § FFS 2005:2

Biträdande signalskyddschef bör även utses vid myndighet eller enhet med omfattande signalskyddsverksamhet.

En myndighet eller enhet som endast innehar system för aktiva kort får i stället för signalskyddschef ha en eller flera kortadministratörer. En kortadministratör skall ansvara för administration och redovisning av aktiva kort.

8 § FFS 2005:2

3.3 Ansvar och uppgifter

3.3.1 Signalskyddspersonal

Signalskyddschef

Signalskyddschef leder och samordnar signalskyddstjänsten genom att

- dokumentera signalskyddsverksamheten i instruktion, plan eller annan handling,
- bereda och föredra ärenden rörande signalskyddstjänstens ledning och samordning,
- samordna signalskyddstjänsten med säkerhetsskydds- och IT-säkerhetstjänsterna,
- följa upp signalskyddsläge och aktuellt telehot,
- sammanställa signalskyddsbedömande, order och rapporter samt delge aktuellt signalskyddsläge,
- samverka med berörda myndigheter eller enheter inom signalskyddstjänstens område,
- utarbeta lokala regler och instruktioner för ledning och genomförande av signalskyddsverksamheten,
- upprätthålla signalskyddstjänstens krav på säkerhetsskydd,
- beställa behovet av kryptonycklar och signalskyddsmateriel samt ansvara för dess redovisning,
- tillse att lokal produktion av kryptonycklar genomförs enligt gällande bestämmelser,
- tillse att gällande bestämmelser efterlevs vid förpackning, distribution, driftsättning, delgivning, inventering och förstöring av kryptonycklar,
- vidta erforderliga åtgärder vid signalskyddsincident (kryptonycklar, aktiva kort och/eller materiel),
- tillse att aktiva kort beställs, lämnas ut och följs upp enligt gällande bestämmelser,

- tillse att erforderlig utbildning i signalskydd ges till den personal som skall placeras i signalskyddsbefattning eller nyttja, betjäna eller på annat sätt hantera signalskyddsmateriel, kryptonycklar eller aktiva kort samt att erhållna behörigheter anmäls till TSA,
- tillse att personalens signalskyddsbehörigheter vidmakthålls,
- tillse att lokal utbildning i signalskyddstjänst genomförs av behörig personal samt dokumenteras,
- genomföra internkontroller av signalskyddstjänsten vid egen och underställda enheter.

Beroende på myndighetens eller enhetens storlek samt omfattningen av signalskyddsverksamheten genomför signalskyddschefen tillämpliga delar av ovanstående uppgifter.

Biträdande signalskyddschef

Biträdande signalskyddschef biträder signalskyddschefen i dennes uppgifter.

Systemoperatör

Systemoperatör nyttjar, betjänar och handhar kryptoapparat eller utrustning som innehåller kryptomodul eller krypteringsfunktion samt

- ansvarar för att signalskyddsmateriel och delgivna nycklar hanteras enligt gällande regler,
- bistår signalskyddschefen, beroende på egen kompetens och behörighet, vid utbildning av användare i nyttjande av signalskyddsmateriel,
- deltar i övrig signalskyddstjänst enligt signalskyddschefens bestämmande.

Nyckeladministratör

Nyckeladministratör administrerar kryptonycklar enligt signalskyddschefens bestämmande.

Kortadministratör

Kortadministratör administrerar och ansvarar för redovisning av aktiva kort och certifikat, samt kan efter erforderlig utbildning ges behörighet att hantera och läsa in kryptonycklar, enligt de uppgifter för kortadministratör som framgår av I TST AKT.

3.3.2 Användare

Användare är en person som i telekommunikations- och IT-system, där signalskydd ingår, är behörig att handha signalskyddsmateriel och/eller kryptonycklar. Användare ingår inte i kategorin signalskyddspersonal.

3.4 Dokumentation/planläggning

För att säkerställa signalskyddet och bidra till en hög beredskap inom signalskyddstjänsten krävs det att verksamheten dokumenteras. Detta kan ske i en instruktion alternativt i en särskild plan, arbetsordning eller annan handling. Planläggning av signalskyddstjänsten bör samordnas med övrig planläggning vid myndigheten/enheten.

Underlag för upprättande av instruktion eller motsvarande utgörs av föreskrifter, allmänna råd, instruktioner för signalskyddstjänsten samt tilldelad signalskyddsmateriel och kryptonycklar.

I första hand för militära förband kan även ett signalskyddsbedömande ligga till grund för utarbetandet av instruktion och order för signalskyddstjänsten. Signalskyddsbedömandet syftar till att klarlägga det aktuella hotet och egna möjliga signalskyddsåtgärder. Exempel på disposition av signalskyddsbedömande framgår av bilaga 1.

Vid upprättandet av instruktion för signalskyddstjänsten bör varje myndighet eller enhet noga överväga vilka uppgifter som kan och bör vara offentliga respektive hemliga eller sekretessbelagda. Hemliga eller sekretessbelagda uppgifter bör återfinnas i en H-bilaga. För vägledning vid sekretessbedömning av uppgifter inom signalskyddstjänstens verksamhetsområde se bilaga 2.

Av instruktionen skall framgå omfattning och anknytning till andra instruktioner eller planer, eventuell samordning vid upprättandet samt delgivning inom och utom myndigheten eller enheten. Signalskyddsinstruktionen läggs lämpligen på myndighetens/enhetens interna nät, intranät eller motsvarande. Observera att det dock är direkt olämpligt att lägga ut myndighetens/enhetens signalskyddsinstruktion på Internet.

Varje myndighet som innehar ett signalskyddssystem skall i en handling (instruktion) beskriva signalskyddets organisation vid myndigheten samt ange vilka åtgärder och uppgifter som krävs för att säkerställa signalskyddet. Om myndigheten består av flera enheter gäller detta varje enhet. Instruktionen skall, utöver beskrivningen av signalskyddets organisation, åtminstone innehålla uppgift om

1. de åtgärder som erfordras vid
   – fredstida krishantering och höjd beredskap,
   – mottagning, extern och intern distribution, delgivning, förvaring och förstöring av kryptonycklar, samt
   – signalskyddsincident,

2. myndighetens signalskyddsutbildade personal och dess behörighet,

3. tilldelade nyckelserier och var dessa förvaras samt möjligheten till signalskyddat samband med andra myndigheter,

4. tilldelad signalskyddsmateriel och var den förvaras samt de åtgärder som erfordras vid reparation av materielen, och

5. rutiner för hantering och uppföljning av aktiva kort.

9 § FFS 2005:2

För att sprida kunskap och förståelse för signalskyddstjänsten inom hela myndigheten eller enheten bör de delar som inte är hemliga och som omfattar organisation, uppgifter och resurser inarbetas i allmänt tillgängligt dokument exempelvis arbetsordning, eller motsvarande.

Signalskyddspersonalen skall vara väl förtrogen med och skall delges aktuell dokumentation minst en gång per år.

Myndigheter eller enheter som är samgrupperade bör samordna sin dokumentation och signalskyddsverksamhet.

Utbildning i att dokumentera signalskyddsverksamheten ingår som en del i utbildningen till signalskyddschef. Denna utbildning genomförs vid TSS.

Exempel på instruktion för signalskyddstjänsten framgår av bilaga 3. Underlaget i bilagan kan användas i tillämpliga delar vid dokumentation av signalskyddstjänsten.

Kapitel 4
Utveckling och anskaffning

Vid planering och utformning av ett system för överföring och lagring av information bör det beaktas om och hur signalskydd skall kunna nyttjas i systemet.

Den som avser utveckla eller anskaffa ett signalskyddssystem eller ett IT- eller telekommunikationssystem där kryptografisk funktion avses ingå, skall innan utvecklingen påbörjas samråda med Högkvarteret (TSA).

Under utvecklingen och anskaffningen måste fortlöpande de uppgifter som är av betydelse för säkerheten i systemet dokumenteras.

Utveckling av samt prov och försök med ett signalskyddssystem får endast ske med data som inte omfattas av sekretess (offentliga uppgifter) och om möjligt i sådan driftmiljö som är skild från ordinarie miljö.

Den som ansvarar för utveckling och anskaffning av ett signalskyddssystem tillser att evaluering/säkerhetsgranskning samt att dokumentation av denna genomförs. Principerna för granskningens genomförande samråds med Högkvarteret (TSA).

Högkvarteret ansvarar för utveckling och anskaffning av signalskyddssystem för Försvarsmakten.

En myndighet som utvecklar eller låter utveckla signalskyddsmateriel som är avsedd att ingå i ett system med kryptografiska funktioner för signalskyddsgrad SG TS, SG S eller SG C eller för trafikskydd, skall se till att

1. *materielen konstrueras så att den inte avger röjande signaler (RÖS),*
2. *kryptoalgoritmer och beskrivningar av kryptoalgoritmer inte kommer till obehörigs kännedom,*
3. *kryptoalgoritmer i form av programvara hanteras i fristående datorer och i RÖS-godkänd miljö,*
4. *den som på myndighetens uppdrag erhåller eller utvecklar kryptoalgoritm för användning i ett sådant system förbinder sig att inte utnyttja kryptoalgoritmen, eller del av denna, i annat sammanhang utan skriftligt godkännande av Försvarsmakten, och*
5. *den som avses i punkten 4 förbinder sig att låta myndigheten nyttja kryptoalgoritmen, och dess källkod, för att kontrollera att den fungerar på önskat sätt och att kunna utveckla kryptoalgoritmen på det sätt signalskyddet kräver.*

26 § FFS 2005:2

En myndighet som upphandlar signalskyddsmateriel, eller programvara för sådan materiel, som har avgörande betydelse för att den totala säkerheten i systemet upprätthålls skall se till att leverantören genom avtal förbinder sig att följa regler för hantering och förvaring av signalskyddsmateriel.

27 § FFS 2005:2

För att ett system skall kunna bli godkänt som signalskyddssystem ställs specifika krav. I bilaga 4 redovisas övergripande krav som måste

uppfyllas vid utveckling och/eller upphandling av system som nyttjar kryptografiska funktioner som skyddsmekanism vid hantering av hemliga uppgifter.

Anskaffning av signalskyddsmateriel sker normalt genom att respektive myndighet/enhet, i samråd med Högkvarteret (TSA), ger FMV uppdrag att genomföra anskaffningen. All utveckling och anskaffning skall om möjligt samordnas inom totalförsvaret.

Uppdrag om utveckling och anskaffning av signalskyddsmateriel för Försvarsmakten samordnas av Högkvarteret. Detta innebär att enskilt projekt eller motsvarande *inte* utan samråd med ansvarig vid Högkvarteret (TSA) får ställa uppdrag om utveckling och anskaffning. Se även avsnitt 6.6.1 ”Rutiner vid upphandling och utveckling”.

4.1 Ansvar och uppgifter

4.1.1 Försvarsmakten

Totalförsvarets signalskyddssamordning i Högkvarteret

- deltar i utveckling och samordning vid anskaffning av signalskyddsmateriel ingående i gemensamma signalskyddssystem avsedda för totalförsvaret,
- granskar och godkänner system med kryptografiska funktioner och system för skydd mot signalspaning, störsändning och falsk signalering,
- utvecklar, anskaffar och granskar program och materiel för produktion och distribution av kryptonycklar, aktiva kort och mjuka certifikat.

Högkvarteret

- fastställer och anskaffar behovet av signalskyddsmateriel ingående i gemensamma och funktionsspecifika signalskyddssystem avsedda för Försvarsmakten,
- samordnar, i samråd med TSA, utveckling av materiel ingående i funktionsspecifika signalskyddssystem avsedda för Försvarsmakten.

4.1.2 Försvarsmakten närstående myndigheter

Försvarets materielverk (FMV), Försvarets radioanstalt (FRA), Försvarshögskolan (FHS), Totalförsvarets forskningsinstitut (FOI), Totalförsvarets pliktverk (PliktV) och Fortifikationsverket (FORTV) fastställer och anskaffar behovet av materiel ingående i gemensamma signalskyddssystem till respektive myndighets organisationsenheter, vad avser Försvarets materielverk även till försvarsindustrin.

Ovanstående gäller om inte annat framgår av författning eller avtal mellan Försvarsmakten och respektive myndighet.

4.1.3 Krisberedskapsmyndigheten

Samordnar civila försvarets krav vid utveckling av totalförsvarsgemensamma signalskyddssystem.

Fastställer och anskaffar behovet av materiel ingående i gemensamma signalskyddssystem avsedda för riksdagen, regeringskansliet samt till civila myndigheter/enheter utom till Försvarsmakten närstående myndigheter enligt ovan.

4.1.4 Respektive myndighet

Materiel som är avsedd att ingå i en myndighets/enhets funktionsspecifika signalskyddssystem utvecklas, fastställs och anskaffas, i samråd med TSA, av respektive myndighet.

Kapitel 5
Utbildning

En grundläggande förutsättning för ett effektivt signalskydd är att all berörd personal får utbildning i signalskydd.

> *Varje myndighet skall se till att den personal som nyttjar, betjänar eller på annat sätt hanterar telekommunikations- och IT-system har kunskap om hur dessa system kan hotas genom avsiktlig eller oavsiktlig obehörig insyn eller påverkan.*
>
> 2 § FFS 2005:2

En väl genomförd utbildning är ett effektivt sätt att höja säkerhetsnivån vid användning av telekommunikations- och IT-system. Förståelse och kunskap om hotet ökar motivationen för att nyttja signalskydd. Utbildningen i signalskydd bör därför inte bara omfatta signalskyddspersonal och användare av signalskyddssystem, utan även en anpassad utbildning för chefer, projektledare, utvecklingspersonal, säkerhetsadministratörer, underhålls- och förrådspersonal m fl.

Högkvarteret (TSA) inriktar signalskyddsutbildningen inom totalförsvaret. Inriktning av signalskyddsutbildningen för civila myndigheter sker i samråd med KBM.

I enlighet med Högkvarteret (TSA) inriktning leder och samordnar chefen för TSS signalskyddsutbildningen inom totalförsvaret. För sådan utbildning fastställer TSS utbildningsmål samt tillhandahåller utbildningsplaner och utbildningsunderlag. TSS utbildningsunderlag bör användas vid all utbildning.

Försvarsmaktens skolor och förband samt övriga som bedriver signalskyddsutbildning biträder TSS vid framtagning av utbildningsmål, utbildningsplaner och utbildningsunderlag.

Den som utbildar i signalskydd skall ha behörighet för detta enligt särskilt behörighetsbevis.

Behörighetsbevis får endast utfärdas av Försvarsmakten och av den som av Försvarsmakten har godkänts som utbildare i signalskydd.

11 § FFS 2005:2

För signalskyddslärare och signalskyddschefer skall sådant behörighetsbevis utfärdas av chefen för TSS eller den han/hon utser.

Säkerhetskrav, utbildningskrav m m vid uttagning av signalskyddspersonal och användare framgår av avsnitt 3 ”Ledning”.

5.1 Genomförande

TSS signalskyddsutbildning omfattar till sin huvuddel signalskyddschefs-, signalskyddslärar- och kortadministratörsutbildning för det militära och civila försvaret samt systemoperatörsutbildning för civila myndigheter.

Signalskyddsutbildning kan även genomföras vid andra enheter som har behörig signalskyddslärare eller annan behörig utbildare i signalskydd, exempelvis Försvarsmaktens skolor/förband som till sin huvuddel utbildar värnpliktig personal. Vid behov kan signalskyddsutbildning för civila myndigheter även genomföras vid dessa skolor/förband.

Efter genomförd och godkänd utbildning erhålls behörighet att inneha befattning som signalskyddspersonal under begränsad tid. Sådan behörighet utfärdas av C TSS vid kurser enligt TSS kurskatalog. Vid kurser som genomförs lokalt utfärdar signalskyddslärare behörighet vid egen myndighet/enhet eller förband.

Utnämning av signalskyddschefer i befattning görs av myndighets-, enhets-, eller förbandschef.

Vid egen myndighet/enhet eller förband genomförs normalt utbildning av användare och nyckeladministratörer. Sådan utbildning skall ges av person som givits behörighet enligt 11 § FFS 2005:2.

Planerade kurser tillkännages årligen i TSS kurskatalog, med undantag för kurser på myndighets-/enhets- eller förbandsnivå.

5.1.1 Signalskyddspersonal

Signalskyddsutbildning bedrivs som grundutbildning och repetitionsutbildning samt som kompletterande utbildning vid införande av nya system. Grundutbildningen syftar till att ge eleven den kunskap som erfordras för att kunna tjänstgöra i avsedd befattning. Repetitions- och kompletteringsutbildning syftar till att genom förnyad utbildning vidmakthålla och öka elevens kunskap.

Kunskapen bör även bibehållas genom regelmässig användning av tilldelade signalskyddssystem och deltagande i kryptotrafikövningar samt deltagande i centrala/regionala signalskyddsmöten.

För att säkerställa signalskyddsberedskapen inom totalförsvaret samt för att öka färdigheten bör signalskyddsutbildad personal minst två gånger per år beredas tillfälle att delta i kryptotrafikövningar. Övningarna bör genomföras på ett sådant sätt att deltagarna övas i exempelvis felsökning, expeditionshantering och signalskyddstjänstens bestämmelser.

För att möjliggöra en likartad tillämpning av regler och instruktioner för signalskyddstjänsten inom totalförsvaret bör det i en signalskyddsutbildning ingå:

- Hur telekommunikations- och IT-system kan hotas genom avsiktlig eller oavsiktlig obehörig insyn eller påverkan.
- Signalskyddets organisation, uppgifter och regelverk.
- Aktuell befattnings ansvar och uppgifter.
- Signalskyddstjänstens säkerhetsskydd främst avseende hantering, förvaring och förstöring av kryptonycklar samt hantering och förvaring av signalskyddsmateriel.

Signalskyddschef

Utbildning av signalskyddschefer för samtliga organisatoriska nivåer sker vid TSS. Efter avslutad utbildning erhålls behörighet att verka i befattning som signalskyddschef samt behörighet att, inom egen organisation, utbilda nyckeladministratörer och användare i kryptonyckelhantering. Dessutom erhålls behörighet att vidareutbilda systemoperatörer till biträdande signalskyddschefer.

Förvärvad behörighet gäller i tre år under förutsättning att personen under tiden tjänstgör i signalskyddsbefattning. För att bibehålla sin behörighet skall signalskyddschef genomgå kompletterande utbildning. Ett annat sätt att bibehålla sin behörighet efter genomförd utbildning är att signalskyddschefen deltar i signalskyddsmöte arrangerat av FM och KBM minst en gång vartannat år.

För att kunna tillgodogöra sig utbildningen skall en blivande signalskyddschef ha genomgått utbildning i säkerhetsskyddstjänst samt uppfylla förkunskapskraven enligt TSS kurskatalog.

Biträdande signalskyddschef

Någon centraliserad utbildning till biträdande signalskyddschef genomförs normalt inte. Vid behov av biträdande signalskyddschef, utser respektive myndighet/enhet lämplig person som genomgått utbildning till signalskyddschef alternativt systemoperatör. Myndighetens/enhetens signalskyddschef ansvarar för att den blivande biträdande signalskyddschefen får erforderlig utbildning.

Systemoperatör

Utbildning av systemoperatörer sker vid TSS eller vid myndighet/enhet eller förband som har behöriga signalskyddslärare. Efter avslutad utbildning erhålls behörighet att verka i befattning som systemoperatör på de system som ingått i utbildningen.

Förvärvad behörighet bibehålls genom regelbunden användning av aktuella signalskyddssystem, deltagande i kryptotrafikövningar eller förnyad utbildning enligt signalskyddschefens bedömande.

Systemoperatör kan erhålla behörighet att utbilda användare inom egen organisation i användning av signalskyddsmateriel som ingått i systemoperatörsutbildningen. Behörigheten gäller dock inte kryptonyckelhantering. Utbildningsbehörighet ges normalt inte till värnpliktig personal.

För att kunna tillgodogöra sig utbildningen skall en blivande systemoperatör ha genomgått utbildning i säkerhetsskyddstjänst samt uppfylla förkunskapskraven enligt TSS kurskatalog.

Nyckeladministratör

Någon centraliserad utbildning till nyckeladministratör genomförs normalt inte. Vid behov av nyckeladministratör utser respektive myndighet/enhet lämplig person som genomgått säkerhetsskyddsut-

bildning. Myndighetens/enhetens signalskyddschef ansvarar för att erforderlig utbildning ges i kryptonyckelhantering. TSS utbildningsunderlag bör användas.

Kortadministratör

Utbildning av kortadministratörer för aktiva kort och mjuka certifikat genomförs av TSS. Efter avslutad utbildning erhålls behörighet att verka som kortadministratör samt behörighet att utbilda användare i hantering av aktiva kort och/eller mjuka certifikat med tillhörande handlingar.

Förvärvad behörighet bibehålls genom att regelbundet verka som kortadministratör eller förnyad utbildning enligt signalskyddschefens bedömande.

För att kunna tillgodogöra sig utbildningen skall en blivande kortadministratör ha genomgått utbildning i säkerhetsskyddstjänst samt uppfylla förkunskapskraven enligt TSS kurskatalog.

5.1.2 Övrig personal

Signalskyddslärare

Utbildning av signalskyddslärare sker vid TSS. Efter avslutad utbildning erhålls behörighet att verka som signalskyddslärare och genomföra grund- och systemutbildning i signalskydd.

Förvärvad behörighet gäller i tre år under förutsättning att personen under tiden tjänstgör som signalskyddslärare. För att bibehålla sin behörighet skall signalskyddslärare genomgå kompletterande utbildning. Ett annat sätt att bibehålla sin behörighet efter genomförd utbildning är att signalskyddsläraren deltar i signalskyddslärarmöte minst en gång vartannat år.

För att kunna tillgodogöra sig utbildningen skall en blivande signalskyddslärare ha genomgått utbildning i säkerhetsskyddstjänst samt uppfylla förkunskapskraven enligt TSS kurskatalog.

Användare

Dagens IT-system medför att allt fler i sitt dagliga arbete använder kryptoapparater eller utrustningar som innehåller kryptografiska funktioner. För att garantera att signalskyddsmateriel och kryptonycklar hanteras på ett för signalskyddstjänsten riktigt och säkert sätt, krävs utbildning även för denna grupp av personal.

Någon centraliserad utbildning för användare genomförs normalt inte. Myndighetens/enhetens signalskyddschef ansvarar för att erforderlig utbildning i säkerhetsskydd, kryptonyckelhantering och handhavande av aktuell utrustning ges till den blivande användaren. Efter avslutad utbildning erhålls behörighet att nyttja aktuellt signalskyddssystem.

Förvärvad behörighet bibehålls genom regelbunden användning av aktuella signalskyddssystem, deltagande i kryptotrafikövningar eller förnyad utbildning enligt signalskyddschefens bedömande.

Underhållspersonal

Underhållspersonal, såsom tekniker, konsulter och/eller installatörer som skall hantera, reparera eller installera signalskyddsmateriel skall utöver den rent tekniska utbildningen även ha utbildning som systemoperatör. Efter avslutad utbildning erhålls behörighet att verka i aktuell befattning.

Förrådspersonal

Förrådspersonal skall ha genomfört utbildning i hantering av signalskyddsmateriel. Myndighetens/enhetens signalskyddschef ansvarar för att utbildning i säkerhetsskydd och handhavande av signalskyddsmateriel ges. Utbildning sker vid myndighet/enhet av behörig signalskyddschef/signalskyddslärare. Efter avslutad utbildning erhålls behörighet att hantera signalskyddsmateriel.

5.2 Dokumentation av genomförd utbildning

Behörighetsbevis på genomförd signalskyddsutbildning skall överlämnas till elev snarast efter det att utbildningen avslutats. Genomförd utbildning skall i skrivelse meddelas till elevanmälande myndighet/enhet samt vad avser signalskyddschefer och kortadministratörer även till Högkvarteret (TSA). Av behörighetsbevis och skrivelse skall det framgå vilka behörigheter som erhållits.

Varje myndighet/enhet skall enligt vad som framgår av 9 § punkten 2 FFS 2005:2 i en handling (instruktion) förteckna myndighetens/enhetens signalskyddsutbildade personal och dess behörighet. Observera att detta även gäller den personal som utbildats vid den egna organisationsenheten (se även avsnitt 3.4 ”Dokumentation/planläggning”).

Av förteckningen skall framgå

- kursanordnande skola eller lokal utbildare,
- förteckning över vilka signalskyddssystem utbildningen omfattade,
- omfattning av övrig signalskyddsutbildning,
- tidpunkten för genomförandet.

Centralt register

TSS upprätthåller centralt register över all behörig personal som utbildats till signalskyddschef, systemoperatör, kortadministratör och signalskyddslärare.

Myndighet/enhet eller förband som genomfört lokal utbildning av systemoperatörer bör senast två veckor efter genomförd utbildning rapportera detta enligt anvisningar från TSS.

Kapitel 6
Signalskyddssystem

Ett signalskyddssystem består av signalskyddsmateriel, kryptonycklar och/eller aktiva kort samt instruktion för systemets hantering.

Om obehörig får tillräcklig kunskap om använt signalskyddssystems konstruktion och tillgång till använd kryptonyckel, kan alla tillgängliga meddelanden skyddade med detta system och med denna nyckel dekrypteras eller tolkas av obehörig.

Om obehörig får tillgång till aktivt kort möjliggörs otillbörligt intrång, förfalskning eller förändring av signerat dokument. Dessutom kan hemlig eller sekretessbelagd information röjas, exempelvis kryptonycklar.

För att säkerställa att ett signalskyddssystem ger avsett skydd mot obehörig åtkomst (sekretesskydd) och förvanskning (integritetsskydd) samt att erforderlig signalskyddsmateriel är tillgänglig och fungerar (tillgänglighet) vidtas åtgärder för att

- förhindra tillgrepp eller obehörig åtkomst av kryptonycklar,
- förhindra tillgrepp eller obehörig åtkomst av aktiva kort och dess olika PIN och PUK,

- förhindra manipulation eller tillgrepp av signalskyddsmateriel,
- försvåra avlyssning av röjande signaler från telekommunikationssystem och IT-system anslutna till signalskyddsutrustning.

Vidare bör den som tilldelats signalskyddssystem avdela tillträdesskyddade utrymmen där verksamheten kan bedrivas, så att obehöriga inte ges möjlighet att ta del av sekretessbelagd information eller sprida falska meddelanden i våra telekommunikations- och IT-system.

Varje myndighet som har anskaffat eller tilldelats ett signalskyddssystem skall följa de instruktioner som Högkvarteret meddelar i fråga om användningen av systemet.

6 § FFS 2005:2

6.1 Benämning och beteckning

Signalskyddssystem benämns och indelas i gemensamma och funktionsspecifika system.

Gemensamma system är de system som utvecklats för gemensam användning i flera olika telekommunikations- och/eller IT-system. Beteckning på sådana signalskyddssystem fastställs av Högkvarteret (TSA).

Funktionsspecifika system är de system som utvecklats för en viss funktion och som inte är gemensamma. Beteckning på sådana system fastställs av TSA i samråd med systemansvarig civil myndighet/enhet eller ledning i Högkvarteret.

Ovanstående system benämns och indelas vid behov i kryptosystem, täcksystem, engångskod, anropssignalsystem, lösensystem och autentiseringssystem.

För att upplysa om ett systems typ och användningsområde m m betecknas dessa med två, tre eller fyrställig beteckning.

Krypto- och lösensystem

Beteckningen på krypto- och lösensystem består normalt av tre tecken som anges med bokstäver eller siffror. För system som får användas i internationell verksamhet eller i annan speciell verksamhet som omfattas av särskilda regler, läggs ett fjärde tecken till ursprungsbeteckningen i form av ytterligare en bokstav.

Första tecknet anger hur ett system är utformat.

Tabell 4. Beteckning av kryptosystem

H	för handkryptosystem
M	för maskinkryptosystem
P	för programvarukryptosystem
L	för lösensystem

Andra tecknet anger inom vilket område eller på vilket sätt systemet används.

Tabell 5. Beteckning av kryptosystem

Gemensamma system	
G	För gemensamma system

Funktionsspecifika system	
A	För armésystem
M	För marinsystem
F	För flygvapensystem
C	För civila system
S	För specialsystem
P	För provisoriska system

Tredje tecknet anger i vilken ordning ett system har utvecklats; *A, B..Z, 2 ..9*.

System med treställig beteckning får normalt endast användas inom svenskt territorium. Avvikelse beslutas av Högkvarteret som undantag från gällande bestämmelser.

Fjärde tecknet anger att ett system är framtaget för användning i ett speciellt syfte, t ex internationell verksamhet.

Följande beteckningar används för närvarande, ytterligare tecken tillförs vid behov.

Tabell 6. Beteckning av kryptosystem

A	För system som enbart används för autentisering.
I	För system som är godkända för användning och hantering i internationell verksamhet. Med vederbörliga avtal får systemen även användas och hanteras av utländska medborgare.
U	För system som får användas och hanteras även utrikes, dock endast av personal anställd vid svensk statlig myndighet eller svenskt företag som har tecknat avtal om signalskydd.

Tabell 7. Exempel på kryptosystembeteckning

MGM	**M**askinkrypto	**G**emensamt	typ **M**	
MFCA	**M**askinkrypto	**F**lygvapnet	typ **C**	**A**utentisering
MGSI	**M**askinkrypto	**G**emensamt	typ **S**	**I**nternationell
MGVU	**M**askinkrypto	**G**emensamt	typ **V**	**U**trikes

Täcksystem

Beteckningen på täcksystem kan bestå av två delar.

Första delen anger systemets utformning.

Tabell 8. Beteckning av täcksystem

TT	*T*äck*T*abell
T	*T*äcksystem

Andra delen anger användningsområde.

Tabell 9. Beteckning av täcksystem

A	*A*rmén
M	*M*arinen

Tabell 10. Exempel på täcksystembeteckning

TTA	*T*äck*T*abell	för *A*rmén

6.2 Godkännande

3. signalskyddssystem:

- system med kryptografiska funktioner som är godkänt av Högkvarteret, och

- system för skydd mot signalunderrättelsetjänst, störsändning eller falsk signalering som är godkända av Högkvarteret.

3 § punkten 3 FFS 2005:2

Innan en myndighet använder signalskyddsmateriel i system eller ansluter utrustning till materiel som ingår i ett signalskyddssystem skall myndigheten samråda med Högkvarteret.

5 § FFS 2005:2

För att ett signalskyddssystem skall kunna bli godkänt ställs bl a krav på att kryptoalgoritmen är godkänd, korrekt implementerad och att den används på ett riktigt sätt. Vidare ställs bl a krav på att kryptonycklar i systemet konstrueras, genereras/produceras, distribueras och hanteras på ett säkert och riktigt sätt. Sammanställning av de krav som ställs för ett godkännande av ett system framgår av bilaga 4.

6.2.1 Rutiner för godkännande

Innan ett sådant signalskyddssystem som avses i 3 § punkten 3 FFS 2005:2 (se ovan) får tas i drift måste det vara godkänt av chefen för militära underrättelse- och säkerhetstjänsten i Högkvarteret, eller av den han/hon bestämmer. Ett godkännande dokumenteras i en särskild handling, ”Godkännande av signalskyddssystem XXX”. Exempel samt uppgifter på vad en sådan handling bör omfatta framgår av bilaga 5.

Observera att signalskyddssystem allt oftare ingår som en del i ett annat telekommunikations- eller IT-system. Detta innebär att godkännandet av signalskyddssystemet kommer att ingå som en del av ackrediteringsunderlaget för värdsystemet.

Handläggning

Högkvarteret (TSA) ansvarar för handläggningen inför ett godkännande av ett gemensamt system som utvecklats för användning i olika telekommunikations- och IT-system inom totalförsvaret.

Vid godkännande av ett funktionsspecifikt system, som utvecklats för en viss funktion inom Försvarsmakten, sker handläggningen i samråd med den del av Högkvarteret som givit uppdraget att utveckla systemet.

För de funktionsspecifika system som inte utvecklats med uppdrag från Högkvarteret, exempelvis civila myndigheters system, sker handläggningen inför godkännandet i samråd med den myndighet som givit uppdraget att utveckla systemet.

Driftsättning

Systemägaren ansvarar för att en driftsättning av signalskyddssystemet sker när systemet är godkänt. Vanligtvis är det högkvarteret inom Försvarsmakten och KBM för civila myndigheter, som ansvarar för detta. Driftsättningsskrivelsen reglerar hur systemet skall användas. En fördelning av materielen ingår samt hur underhåll och support skall ske.

Tillgång till det utvecklade systemet

Det är först när systemägaren driftsatt och fördelat det utvecklade signalskyddssystemet som det blir tillgängligt för de behöriga (utbildade) användarna att nyttja systemet.

6.3 Kryptonycklar

Kryptonycklar ingår som en av de viktigaste komponenterna i ett signalskyddssystem och indelas i krypto-, system-, täck-, anrops-, lösen-, autentiserings- och frekvenshoppsnycklar.

Till ovanstående uppräkning skall även tilläggas privat nyckel som ingår i asymmetriska kryptosystem. Den privata nyckeln har signalskyddsgrad SG R och kan lagras på TAK, TEID eller CD märkt hemlig eller signalskyddsgrad SG R.

Beroende på hur en nyckel är avsedd att användas inordnas respektive nyckel i en av följande huvudgrupper.

Tabell 11. Typvarianter av kryptonycklar

Gemensam nyckel	Nyckel som finns i två eller flera exemplar.
Grundnyckel	Nyckel som används för att kryptera kommunikationen mellan användare och nyckelserver.
Personlig nyckel	Nyckel som endast finns i ett exemplar för personligt bruk, t ex i hårddiskkrypto.

Kryptonycklars data kan lagras på följande nyckelmedia.

- Blankett med streckkod eller med alfanumeriska tecken.
- Aktivt kort.
- Elektroniskt minne, t ex nyckelinjektor.
- Optiskt lagringsmedium, t ex CD.
- Hålkort.

För att ett signalskyddssystem skall ge avsett skydd krävs att dess kryptonycklar förvaras på ett sådant sätt att tillgrepp eller obehörig åtkomst förhindras och att nycklarna i övrigt hanteras på sådant sätt att sekretessen kring dessa aldrig kan ifrågasättas. Observera att detta gäller speciellt för kryptonycklar som har varit i bruk och upphört att gälla, då dessa har lika högt sekretessvärde och minst lika högt underrättelsevärde som en gällande nyckel.

Kryptonycklar är hemliga eller sekretessbelagda om inte annat anges. Nycklarna får *inte* hanteras av personal som *saknar* erforderlig utbildning i signalskydd. Regler för utbildning framgår av avsnitt 5 ”Utbildning”.

Frågor som rör en begäran från obehörig att få ta del av kryptonyckel måste prövas i samråd med nyckelansvarig och Högkvarteret (TSA).

6.3.1 Märkning och beteckning

För att upplysa om en nyckels användningsområde, giltighetstid m m är nycklarna i förekommande fall märkta med

- signalskyddssystem,
- nyckelserie,
- lottningsnummer,
- giltighetstid,
- kryptobeteckning,
- signalskyddsgrad eller trafikskydd,
- hemligbeteckning och exemplarnummer,
- färg.

Signalskyddssystem

Symmetriska kryptonycklar är märkta med en systembeteckning, som består av 3 eller 4 tecken, för att visa vilket system en viss nyckel tillhör. Principer för uppbyggnad av systembeteckningar framgår av avsnitt 6.1 ”Benämning och beteckning”.

Exempel: **MGA** ……

Nyckelserie

För att minska risken för forcering och för att begränsa skadeverkningarna om en kryptonyckels nyckelinformation kommer till obehörigs kännedom, delas nycklarna in i olika serier. En nyckels seriebeteckning omfattas normalt av sekretess. Indelningen sätts i relation till ett bestämt användningsområde, t ex att nyckelserien skall användas inom en viss organisation, funktion eller under ett visst skede.

Beteckningen för en nyckelserie (seriebeteckning) delas upp i 4 delar och anges på nyckeln efter systembeteckningen.

Nyckelseriens första del anger vem som är nyckelansvarig och betecknas med vedertagen förkortning för den myndighet eller enhet som är nyckelansvarig.

Nyckelseriens andra del anger användningsområde eller funktion.

Nyckelseriens tredje del anger under vilket skede eller verksamhet nyckeln är avsedd att användas.

Nyckelseriens fjärde del utgör i förekommande fall tilläggsinformation.

Vilken beteckning en viss nyckelserie skall ha fastställs av nyckelansvarig i samråd med Högkvarteret (TSA).

Lottningsnummer

I anslutning till en nyckels system- och seriebeteckning anges ett lottningsnummer som upplyser användaren om i vilken ordning respektive nyckel i en serie skall tas i bruk.

Giltighetstid

En kryptonyckel kan gälla för en bestämd tid eller för kryptering av en bestämd mängd information. Styrande är användningsskede och användningsområde samt nyckelns spridning.

För att ange en nyckels giltighetstid i klartext, märks den i anslutning till lottningsnumret med datum (åååå-mm-dd eller åå-mm-dd) och i förekommande fall klockslag (ttmm-ttmm) när den skall börja respektive upphöra att gälla.

Kryptobeteckning

I anslutning till nyckelns system- och seriebeteckning anges i förekommande fall kryptobeteckning (krybet). Krybet anges traditionellt med fem tecken. För vissa system med många nyckelserier består krybet av åtta tecken. Krybet anger i kodad form en nyckels identitet. Kryptobeteckningen omfattas ej av sekretess.

Signalskyddsgrad

Angiven signalskyddsgrad ger viss vägledning om hur nyckeln skall hanteras samt vilken information som nyckeln är godkänd för att skydda. Se avsnitt 2.1 ”Signalskyddsgrader”.

Trafikskydd

Angiven märkning ger viss vägledning om hur nyckeln skall hanteras och att denna nyckel skall användas för trafikskydd. Kryptonyckel märkt trafikskydd är ej avsedd för sekretesskydd.

Hemligbeteckning och exemplarnummer

Kryptonycklar är märkta med hemligbeteckning och exemplarnummer enligt reglerna för märkning av hemlig handling. Exemplarnummer återfinns normalt i nyckelns övre högra hörn.

Färgmärkning

För att tydliggöra under vilket skede eller verksamhet en nyckel är avsedd att användas är den märkt med en viss färg enligt tabellen nedan.

Tabell 12. Färgmärkning av kryptonycklar

Beredskapsnyckel	Gul
Freds-/Beredskapsnyckel	Vit
Fredsnyckel	Vit
Utbildningsnyckel	Grön
Testnyckel	Orange
Tillfällig övningsnyckel	Rosa

6.3.2 Nyckelansvar

Nyckelansvarigs uppgift är att operativt och administrativt ansvara för kryptonycklar som ingår i en bestämd nyckelserie vad avser

- fastställande av beteckning och tilldelning,
- driftsättning,
- vem som får ta del av en nyckel,
- behovet av ersättningsnycklar,
- åtgärder vid höjd beredskap,
- åtgärder i samband med nyckelincident, se avsnitt 6.3.13,
- tillfällig ändring av giltighetstid,
- tillstånd att mångfaldiga kryptonyckel,
- avveckling av kryptonyckelserie.

Vem som är nyckelansvarig för en kryptonyckelserie ingående i ett visst system framgår normalt av kryptonyckelns seriebeteckning.

De nyckelansvariga myndigheter som har tillgång till redovisningssystemet IS UNDSÄK TSA, rutin NAM, skall använda systemet vid administration som rör utövandet som nyckelansvarig myndighet.

6.3.3 Tilldelning av nyckelserie

Nyckelansvarig fastställer för varje systems nyckelserie, i samråd med Högkvarteret (TSA) och berörda myndigheter eller enheter, vilka militära och/eller civila enheter som skall tilldelas nyckelserien. Tilldelningen fastställs i en särskild skrivelse som delges de enheter som skall tilldelas serien samt de enheter som har ansvaret för att beräkna och beställa behovet av kryptonycklar.

Innan tilldelningen av en nyckelserie fastställs skall nyckelansvarig kritiskt pröva behovet av den aktuella seriens spridning. Principen skall vara att *varje nyckelserie skall ha minsta möjliga spridning*. Detta för att begränsa skadeverkningarna om en kryptonyckels nyckelinformation kommer till obehörigs kännedom.

6.3.4 Beställning av nycklar

Med tilldelade nyckelserier som underlag beräknas och beställs behovet av antalet nycklar för respektive serie.

Regeringskansliet

Regeringskansliet beräknar och beställer kryptonycklar dels för eget behov och dels för Riksdagen. Det samlade behovet beställs vid Högkvarteret (TSA).

Försvarsmakten

Försvarsmaktens förband, skolor och centra sammanställer och beställer sitt samlade behov av kryptonycklar vid Högkvarteret (TSA).

För Försvarsmaktens förband utomlands gäller särskilda bestämmelser.

Försvarsmakten närstående myndigheter

FMV beräknar och beställer kryptonycklar för eget behov och för försvarsindustrin. Det samlade behovet beställs vid Högkvarteret (TSA).

FRA beräknar och beställer kryptonycklar för eget behov inklusive FRA:s regionala enheter. Det samlade behovet beställs vid Högkvarteret (TSA).

Försvarshögskolan, Totalförsvarets forskningsinstitut och Fortifikationsverket beräknar och beställer kryptonycklar för eget behov. Det samlade behovet beställs vid Högkvarteret (TSA) om inte annat har överenskommits.

Krisberedskapsmyndigheten (KBM)

KBM beräknar och beställer kryptonycklar för eget behov och för civila centrala myndigheter (som inte beställer sitt eget behov vid Högkvarteret) inklusive deras regionala och lokala enheter samt för företag som tilldelats nyckelserie. Det samlade behovet beställs vid Högkvarteret (TSA).

Övningsanordnande myndighet, förband eller skola

Beräknar och beställer nycklar för de enheter som skall delta i övning där tillfälliga övningsnycklar (TIFÖ-nycklar) skall användas. Det samlade behovet för övningen beställs vid den organisationsenhet som normalt distribuerar ordinarie nycklar.

Regler för beställning

Ordinarie nycklar

Förändringar i behovet av kryptonycklar anmäls fortlöpande av respektive signalskyddschef till den som ansvarar för beställning. Ansvariga för beställning sammanställer behoven och beställer det totala behovet vid Högkvarteret (TSA) eller vid den enhet som ansvarar för produktionen av de aktuella nycklarna.

Vid beställning av freds- och fred/beredskapsnycklar skall hänsyn tas till att antalet kryptonycklar även skall tillgodose behovet vid en eventuell beredskapshöjning med fredsorganisationens resurser.

Beställning/avbeställning bör om möjligt göras i redovisningssystemet för kryptonycklar (IS UNDSÄK TSA). För de enheter som inte har tillgång till IS UNDSÄK görs beställningen på fastställd blankett. Blanketten kan beställas från Högkvarteret (TSA).

Observera att ifylld blankett för *beställning av kryptonycklar är hemlig handling* såvida beställningen inte enbart rör ej sekretessbelagda test- och utbildningsnycklar.

Utbildningsnycklar

Utbildningsnycklar är ej sekretessbelagda och beställs direkt vid Högkvarteret (TSA).

Testnycklar

Testnycklar är ej sekretessbelagda och levereras normalt tillsammans med respektive systeminstruktion eller signalskyddsutrustning. Vid behov av ytterligare testnycklar beställs dessa direkt vid Högkvarteret (TSA).

Tillfälliga övningsnycklar

Behovet av TIFÖ-nycklar beställs av den som ansvarar för övningen. Det samlade behovet för övningen beställs vid den organisationsenhet som normalt distribuerar ordinarie nycklar. Beställning sker enligt samma principer som för ordinarie nycklar enligt avsnitt 6.3.4 ”Beställning av nycklar”.

Vid fastställande av nyckelserie och vid beställning av TIFÖ-nycklar anges övningens namn, övningsdatum och önskat förpackningssätt. Normalt är förpackningssättet detsamma som för motsvarande ordinarie nycklar.

Beställning av TIFÖ-nycklar till försvarsmaktsövning eller övning inom det civila försvaret av motsvarande omfattning, bör vara Högkvarteret (TSA), eller den enhet som ansvarar för produktionen av de aktuella nycklarna, tillhanda *senast sex månader före* önskat leveransdatum. Beställningar för mindre övningar bör vara producerande enhet tillhanda senast två månader före önskat leveransdatum.

6.3.5 Nyckelproduktion

Kryptonycklar produceras normalt vid Högkvarteret (TSA). I samråd med nyckelansvarig och efter särskilt beslut av Högkvarteret (TSA) kan delar av nyckelproduktionen förläggas till annan myndighet/enhet, förband eller skola inom totalförsvaret.

> *En myndighet som producerar kryptonycklar får endast använda utrustning, programvara och metoder som har godkänts av Högkvarteret.*
>
> *Produktion av kryptonycklar får endast ske på sådant sätt att obehöriga inte får insyn i verksamheten.*
>
> 15 § FFS 2005:2

Programvara som är avsedd att användas vid produktion av SG R-kryptonycklar skall förvaras på ett sådant sätt att obehörig hantering och tillgrepp förhindras. Övriga programvaror för produktion av kryptonycklar är normalt hemliga.

Endast utrustning som inte avger röjande signaler (RÖS) får användas vid produktion av kryptonycklar, om inte annat framgår av respektive systemgodkännande. Utrustningen får inte heller förvaras så obehöriga har möjlighet att manipulera den.

Utrustning i vilken kryptonycklar, utom sådana nycklar som är märkta med signalskyddsgrad SG R, läses in, förvaras, produceras eller används får inte vara konstruerad på ett sådant sätt eller innehålla programvara som möjliggör att nycklarna kan mellanlagras i klartext på permanenta minnesmedia, såsom diskett eller hårddisk.

14 § FFS 2005:2

Vid produktion av kryptonycklar, som inte enbart existerar i elektronisk form, skall varje enskilt exemplar märkas med uppgift om vilket signalskyddssystem nyckeln är avsedd för, nyckelserie, giltighetstid, lottningsnummer och signalskyddsgrad samt i förekommande fall kryptobeteckning. Kryptonycklar skall även förses med hemligbeteckning (hemligstämpel) och exemplarnummer.

Produktion av sådana kryptonycklar som avses i första stycket skall dokumenteras. Av dokumentationen skall framgå vilket signalskyddssystem nyckeln är avsedd för, nyckelserie, nyckelns giltighetstid, dess lottningsnummer och exemplarnummer. Dokumentationen skall sparas i minst 10 år efter det att respektive nyckel har upphört att gälla.

Endast den som är nyckelansvarig får besluta att avskrift eller kopia av kryptonyckel får göras. Det skall framgå av avskriften eller kopian hur många exemplar som har framställts.

16 § FFS 2005:2

Utdrag ur anropsnyckel i form av anropssignaler för enstaka enheter får dock göras utan tillstånd från nyckelansvarig.

Krypteringsapparat försedd med inbyggd nyckellottningsfunktion kan användas för lokal produktion av kryptonycklar. Vid lokal produktion skall seriebeteckning med bokstäverna YA-YZ väljas.

Vid utveckling av produktionsprogram för kryptonycklar skall för varje nyckeltyp arkiveras ett provexemplar som utvisar konstruktion och utformning av kryptonyckeln. Likaså arkiveras ett exemplar av sådan kryptonyckel som utvisar förändring i fråga om konstruktion och utformning av nyckeln.

6.3.6 Kopiering och mångfaldigande

Kryptonycklar får normalt inte kopieras eller mångfaldigas. Kryptonycklar får endast undantagsvis kopieras/mångfaldigas efter beslut av nyckelansvarig som också meddelar hur och med vilka metoder och med vilken utrustning kopiering/mångfaldigande får ske. Observera att mellanlagring av kryptonycklar ej är tillåtet på permanent lagringsmedia (t ex kopiators hårddisk). Undantag kan dock göras för kryptonycklar märkta med signalskyddsgrad SG R, vilket i så fall framgår av systemgodkännandet.

6.3.7 Förpackning och distribution

Varje myndighet skall se till att erforderliga skyddsåtgärder vidtas vid distribution av kryptonycklar.

17 § FFS 2005:2

Distribution av kryptonycklar via telekommunikation får inte ske utan tillstånd av den som är nyckelansvarig.

18 § första stycket FFS 2005:2

Beslut om sådant tillstånd bör tas i samråd med Högkvarteret (TSA). Avsändaren måste vid sådan distribution förvissa sig om att mottagaren är behörig. Distributionen får endast ske med system som är godkänt för högre signalskyddsgrad.

För system som är särskilt framtagna och avsedda för att distribuera nycklar elektroniskt gäller särskilda regler enligt respektive instruktion.

Kryptonycklar skall försändas i förseglat emballage. Emballaget skall vara så beskaffat att det är omöjligt att ta del av innehållet utan att bryta emballaget. Förseglingen skall vara sådan att det går att se om någon har brutit emballaget.

Det förseglade emballaget skall innehålla ett förseglat innerkuvert, som skall vara försett med påskrift att det innehåller kryptonycklar och att det skall överlämnas obrutet till den som är signalskyddschef eller till den som myndigheten har bestämt.

18 § andra och tredje stycket FFS 2005:2

Försändelser som innehåller kryptonycklar adresseras till myndighet/enhet. Innehållet aviseras som böcker eller blanketter.

Distribution av kryptonycklar, som inte enbart existerar i elektronisk form, skall dokumenteras. Av dokumentationen skall framgå vilket signalskyddssystem nyckeln är avsedd för, nyckelserie, nyckelns giltighetstid, dess lottningsnummer och exemplarnummer samt till vilken myndighet, och i förekommande fall dess enheter, respektive nyckel har distribuerats. Dokumentationen skall sparas i minst 10 år efter det att respektive nyckel har upphört att gälla.

När sådana kryptonycklar som avses i första stycket distribueras skall en följesedel bifogas försändelsen. Följesedeln skall registreras vid mottagandet och sparas i minst 10 år.

Om försändelsen innehåller förproducerade beredskaps- eller ersättningsnycklar skall även kvitto med kopia medfölja försändelsen. Kvittot och kopian skall efter kvittens snarast återsändas till den som har utfärdat kvittot.

19 § FFS 2005:2

Distribution av kryptonycklar bör under grundberedskap ske i så god tid att samtliga myndigheter eller enheter får sina nycklar senast 14 dagar innan de skall börja gälla.

Har kryptonyckel inte kommit användare tillhanda vid den tidpunkt när den skall börja gälla används den kryptonyckel som är i bruk till dess att den nya nyckeln nått användaren. Ändring av giltighetstid enligt ovan anmäls omedelbart till de myndigheter/enheter med vilka kryptosamband upprätthålls samt till nyckelansvarig.

Ansvar för distribution

Den som ansvarar för distribution av kryptonycklar är skyldig att hos nyckelansvarig kontrollera beställarens/mottagarens behörighet till beställd nyckelserie (nyckel), innan nycklarna distribueras.

Högkvarteret

Högkvarteret (TSA) ansvarar för distribution till Regeringskansliet, centrala civila myndigheter samt Försvarsmaktens förband, skolor och centra.

Försvarets materielverk (FMV)

FMV ansvarar för distribution till egna enheter och till försvarsindustrin.

Krisberedskapsmyndigheten (KBM)

KBM ansvarar för distribution till civila regionala och lokala myndigheter och företag samt till de civila centrala myndigheternas regionala och lokala enheter som inte får sina nycklar distribuerade från annan myndighet eller Högkvarteret.

6.3.8 Driftsättning av nyckelserier/nycklar

Av beteckningen för en kryptonyckelserie samt eventuell tilläggsinformation, enligt avsnitt 6.3.1 ”Märkning och beteckning”, framgår under vilket skede eller verksamhet en serie är avsedd att användas.

Nedan anges principerna för driftsättning av nyckelserier avsedda för olika skeden/verksamheter.

FRED (F)

Nyckelserie med beteckning FRED (F) driftsätts av nyckelansvarig i samråd med Högkvarteret (TSA). Vid vilken tidpunkt nycklar ingående i serien skall tas i bruk meddelas av nyckelansvarig. Nycklarna är avsedda att användas under grundberedskap intill dess beredskapsnycklar tas i bruk om inte annat meddelas av nyckelansvarig.

FRED/BER (F/B)

Nyckelserie med beteckning FRED/BER (F/B) driftsätts av nyckelansvarig i samråd med Högkvarteret (TSA). Vid vilken tidpunkt nycklar ingående i serien skall tas i bruk meddelas av nyckelansvarig. Nycklarna är avsedda att användas såväl under grundberedskap som efter höjd beredskap.

BER (B)

Nyckelserie med beteckning BER (B) driftsätts av nyckelansvarig i samråd med Högkvarteret (TSA). Nycklar ingående i serien tas i bruk vid beslut om högsta beredskap eller vid tidpunkt som meddelas av Högkvarteret eller nyckelansvarig. Nycklarna är avsedda att användas efter höjd beredskap om inte annat meddelas av nyckelansvarig.

INTERNATIONELL (INT)

Nyckelserie med beteckning INT driftsätts av nyckelansvarig i samråd med Högkvarteret (TSA). Vid vilken tidpunkt nycklar ingående i serien skall tas i bruk meddelas av nyckelansvarig. Nycklarna är avsedda att användas vid internationell verksamhet.

ERS

Nyckelserie med beteckning ERS driftsätts av nyckelansvarig i samråd med Högkvarteret (TSA). Vid vilken tidpunkt nycklar ingående i serien skall tas i bruk meddelas av nyckelansvarig. Nycklarna är avsedda att användas som ersättning för ordinarie nycklar och gäller enligt direktiv från nyckelansvarig.

Ytterligare instruktioner och metoder för driftsättning av kryptonycklar framgår av särskild instruktion.

6.3.9 Delgivning av nycklar

Signalskyddschef ansvarar för delgivningen av kryptonycklar till systemoperatörer och användare. Signalskyddschefen får vid behov utse och utbilda en eller flera nyckeladministratörer som under signalskyddschefens ledning och ansvar genomför delgivningen.

> *Kryptonycklar får endast delges den som bedöms pålitlig från säkerhetssynpunkt, har tillräckliga kunskaper om säkerhetsskydd, behöver nycklarna för sitt arbete i den verksamhet där de skall hanteras samt har genomgått erforderlig utbildning i nyckelhantering.*
>
> *Signalskyddspersonal som har tillgång till kryptonycklar skall förtecknas. Förteckningen skall sparas i minst 10 år. Övriga som delges kryptonycklar skall kvittera mottagandet. Kvittenslista skall sparas i minst 10 år.*
>
> 20 § FFS 2005:2

Observera att användare ej tillhör kategorin signalskyddspersonal.

Det är mycket viktigt att det vid varje myndighet/enhet finns spårbarhet till den/de som har haft tillgång till viss nyckelserie (nyckel). Detta beaktas särskilt då fler än en person har tillgång till utrymme där kryptonycklar förvaras.

Systemoperatörer och användare får vid ett och samma tillfälle delges och inneha ett begränsat antal kryptonycklar, normalt två lottningar ur samma nyckelserie. Under grundberedskap får dock systemoperatör och användare delges och inneha kryptonycklar för en månads behov, under förutsättning att rutinmässig förstöring, och i förekommande fall radering, sker enligt gällande regelverk (se särskild instruktion).

6.3.10 Hantering och förvaring

För att ett signalskyddssystem skall ge avsett skydd, krävs att dess kryptonycklar hanteras och förvaras på ett sådant sätt att obehörig åtkomst av nycklarna förhindras.

> *Kryptonycklar, utom sådana som är märkta med signalskyddsgrad SG R, skall stå under ständig uppsikt eller förvaras i ett utrymme som uppfyller lägst kraven för säkerhetsskåp enligt Standardiseringskommissionens normer (SIS), Svensk Standard (SS) 3492.*
>
> *Kryptonycklar som är märkta med signalskyddsgrad SG R skall stå under ständig uppsikt eller förvaras på ett sådant sätt att obehörig hantering och tillgrepp förhindras.*
>
> 21 § FFS 2005:2

Observera att även kryptonyckel som är märkt med beteckningen trafikskydd skall stå under ständig uppsikt eller förvaras i ett utrymme som uppfyller lägst kraven för säkerhetsskåp enligt ovanstående standard. Se även 32 § FFS 2005:2 under avsnitt 6.6.6 ”Placering och förvaring”.

> *För att få medföra eller på annat sätt göra kryptonycklar tillgängliga utanför svenskt territorium krävs*
>
> *1. godkännande av Högkvarteret, och*
>
> *2. att den nyckelansvarige i samråd med Högkvarteret har beslutat hur nycklarna skall hanteras.*
>
> 22 § FFS 2005:2

Privata nycklar som ingår i asymmetriska kryptosystem och har signalskyddsgrad SG R (TAK, TEID eller mjuka certifikat) får dock medföras eller på annat sätt göras tillgängliga utanför svenskt territorium utan Högkvarterets godkännande.

Se även avsnitt 9 ”Signalskydd vid internationell verksamhet”.

Ytterligare bestämmelser för hantering och förvaring av kryptonycklar framgår av särskild instruktion.

6.3.11 Redovisning och inventering

Varje myndighet, och i förekommande fall dess enheter, som innehar kryptonycklar skall redovisa dessa till den myndighet, eller enhet, som har distribuerat nycklarna. Redovisningen skall grundas på den följesedel eller det kvitto som medföljer nycklarna när de distribueras.

23 § första stycket FFS 2005:2

De myndigheter/enheter som har tillgång till IS UNDSÄK skall som stöd för sin redovisning använda redovisningssystem för kryptonycklar (IS UNDSÄK TSA).

Förproducerade beredskaps- eller ersättningsnycklar skall inventeras varje år samt vid byte av befattningshavare som ansvarar för sådana nycklar. Inventeringen skall förrättas av signalskyddschefen eller en av myndigheten särskilt utsedd befattningshavare.

Den som har distribuerat förproducerade beredskaps- eller ersättningsnycklar skall inför inventering sända ut ett nytt kvitto (förnyelsekvitto) med kopia. Efter genomförd inventering skall kvittot och kopian snarast återsändas till den som har utfärdat kvittot. Kopian skall sparas i minst 25 år.

23 § andra och tredje stycket FFS 2005:2

Förnyelsekvittots original återsänds till den som genomfört inventeringen efter nästkommande inventering.

Vid inventering får vakuumförsluten nyckelförpackning med förproducerade beredskaps- eller ersättningsnycklar inte brytas för kontrollräkning av innehållet.

Om den vakuumförslutna nyckelförpackningen saknas eller skadats, anmäls detta omgående till den som distribuerat nycklarna. Av anmälan skall framgå vilka som har tagit del av innehållet i nyckelförpackningen. Distributionsansvarig meddelar vilka åtgärder som skall vidtas.

I förekommande fall vidtas åtgärder enligt de rutiner som gäller vid nyckelincident.

Om nyckelförpackning av misstag öppnats skall den omgående återförslutas och händelsen skall omgående anmälas till den som har distribuerat nycklarna.

För att underlätta inventeringen bör det på en enhetsförpackning (se särskild instruktion) framgå vilka nycklar förpackningen innehåller, exempelvis genom kopia på följesedel.

6.3.12 Förstöring och radering

Kryptonycklar som varit i bruk har sannolikt ett mycket högt underrättelsevärde eftersom all information som krypterats med en nyckel kan återskapas med denna nyckel.

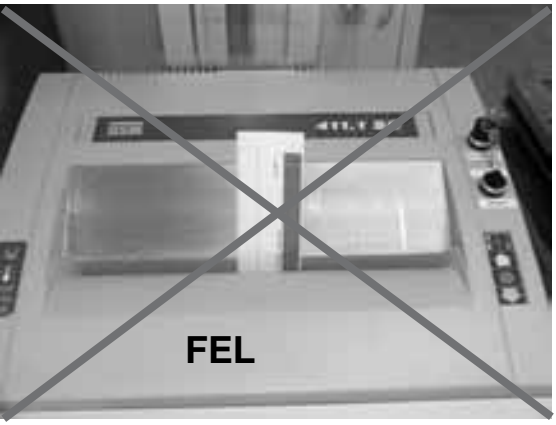
All denna information kan komma obehörig till del om nyckeln kommer i orätta händer. Detta drabbar inte enbart den egna myndigheten/enheten utan alla myndigheter/enheter som använt samma nyckelserie (-lottning). Därför gäller att:

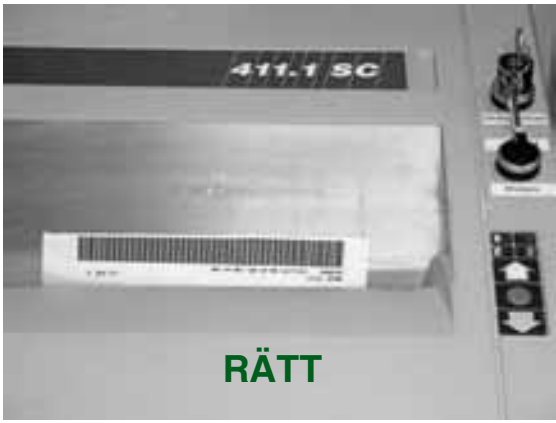
> *Varje kryptonyckel skall förstöras och, i fråga om nycklar som lagras i signalskyddsutrustnings minne, raderas när den har upphört att gälla eller då den inte längre behövs för tjänsten.*
>
> *Förstöringen skall utföras av en person som är utbildad enligt vad som föreskrivs i 10 § och genomföras på ett sådant sätt att åtkomst och återskapande av hela eller delar av nyckeln omöjliggörs. Förstöringen skall dokumenteras. Förstöringsliggare eller motsvarande skall sparas i minst 10 år.*
>
> 24 § FFS 2005:2

Försvarsmakten godkänner två typer av destruktörer. Den ena typen skall ge spån av 2 x 2 mm storlek eller mindre och förordas vid förstöring av kryptonycklar. Den andra typen av destruktör skall ge spån av 15 mm längd och 1,2 mm bredd eller mindre. För att säkerställa att nyckeln inte skall kunna återskapas efter destruktion med denna typ

av destruktör krävs det att kryptonyckel av streckkodstyp matas in på rätt sätt i destruktören enligt nedan. Regler för rutinmässig förstöring framgår av särskild instruktion. Vid förstöring av mjuka certifikat och tillhörande CD se I TST AKT.

Observera att regelbunden funktionskontroll och service av destruktören är en förutsättning för att säkerställa att destruktörens spån håller sig inom godkända måttspecifikationer.





Förstöring av kryptonyckel.

För att säkerställa att obehörig åtkomst och återskapande av hela eller delar av nyckeln omöjliggörs vid användning av destruktör som ger spån av 15 mm längd och 1,2 mm bredd, krävs att nyckeln matas in enligt bilden så att destruktörens knivar skär parallellt med strecken i koden.

Anvisningar för begränsad och total förstöring framgår av bilaga 6. Metoder för omedelbar och hastigt uppkommet behov av förstöring av signalskyddsmateriel, vid t ex internationella missioner, utlandstjänst eller liknande, skall ingå som en del av den ordinarie utbildningen inför en mission eller inför utlandstjänst.

Emballage där kryptonycklar varit förpackade skall förstöras så att emballaget inte kan återanvändas eller innehållet härledas.

6.3.13 Nyckelincident

Kryptering är ett sätt att skydda sig mot obehörig åtkomst av information. Kommer obehörig åt kryptonyckeln har denne möjlighet att ta del av all den information som krypterats med den aktuella nyckeln. En kryptonyckel finns oftast i flera exemplar, dvs den kan användas för kryptering av information som förmedlas till och från flera olika verksamhetsställen. Detta innebär att *om en nyckel blir röjd, drabbar det inte bara ett verksamhetsställe utan alla ställen som använt den aktuella nyckeln*. För att underlätta en framtida menbedömning är det viktigt att trafiklista förs vid samtliga verksamhetsställen för alla utgående meddelanden.

Ovanstående beskrivning vill tydliggöra hur viktigt det är att anmälan görs omedelbart vid nyckelincident och att de åtgärder som måste vidtas sker skyndsamt. Detta för att menet (skadan) skall bli så ringa som möjligt för alla de som har använt den aktuella kryptonyckeln.

Försummelse att omedelbart göra anmälan kan medföra allvarliga negativa följder för rikets säkerhet, för totalförsvarets verksamhet eller för den verksamhet som skall skyddas av den aktuella nyckeln.

Om obehörig har haft möjlighet att ta del av en kryptonyckels nyckelinformation kan nyckeln vara röjd.

> *Den som har förlorat en kryptonyckel, eller misstänker eller på annat sätt har fått uppgift om att en kryptonyckel kan vara röjd, skall omedelbart anmäla detta med ett ilmeddelande till den nyckelansvarige samt, i förekommande fall, till närmast överordnad enhet.*
>
> *Den nyckelansvarige skall avgöra om kryptonyckeln kan ha röjts och meddela de åtgärder som skall vidtas för att återställa signalskyddet.*
>
> 25 § FFS 2005:2

Anmälan är hemlig och signalskyddas, om möjligt, med samma signalskyddsgrad som den misstänkt röjda nyckeln. Anmälan får krypteras med en nyckel som kan vara röjd om annan nyckel inte finns tillgänglig. Av ärendemening i meddelandet får *inte* framgå att anmälan gäller nyckelincident.

För att den som är nyckelansvarig skall ha förutsättning att göra en riktig bedömning och vidta relevanta åtgärder måste en anmälan innehålla åtminstone följande uppgifter.

1. System, serie och giltighetstid/lottningsnummer.
2. Tidpunkt samt under vilka omständigheter nyckeln kan ha röjts.
3. Vid vilken myndighet/enhet nyckeln kan ha röjts.
4. Vidtagna åtgärder.
5. Telefonnummer (krypto) till signalskyddschef eller motsvarande.

För att anmälan skall bli riktig och väl preciserad samt för att undvika att väsentliga uppgifter tappas bort bör den ställas upp i punktform med hänvisning till ovanstående numrering.

Nyckelansvarigs åtgärder

Med underlag av bl a inkommen anmälan avgör nyckelansvarig om kryptonyckel är röjd, kan vara röjd eller icke är röjd. Beroende på vilken bedömning som görs vidtar nyckelansvarig olika åtgärder.

Bedömer nyckelansvarig att nyckeln *kan vara röjd* eller *är röjd* meddelas snarast de åtgärder som krävs för att ta aktuell nyckel ur drift. Vilka åtgärder som nyckelansvarig kan vidta för att återställa det signalskyddade sambandet framgår av särskild instruktion. Åtgärderna meddelas samtliga som tilldelats nyckel ur den aktuella nyckelserien.

I de fall nyckelansvarig har bedömt att en nyckel *är röjd,* och åtgärder vidtagits enligt ovan, överlämnas ärendet till säkerhetsskyddschef eller motsvarande som beslutar om sekretessgranskning för en eventuell menbedömning. Resultatet av sekretessgranskningen utgör underlag för menbedömning.

Av säkerhetsskyddsförordningen (1996:633) föreskrivs följande: ”om en hemlig uppgift kan ha röjts, skall detta skyndsamt anmälas till Rikspolisstyrelsen, om röjandet kan antas medföra men för rikets säkerhet *som inte endast är ringa*.”

I de fall nyckelansvarig har bedömt att en nyckel *kan vara röjd* och åtgärder vidtagits enlig ovan, överlämnas ärendet till säkerhetsskyddschef eller motsvarande som genom en riskanalys gör en riskbedöm-

ning av inträffad händelse. Framkommer det vid riskbedömningen att *det är sannolikt* att obehörig tagit del av kryptonyckelns nyckelinformation, bedöms den aktuella nyckeln som röjd varvid sekretessgranskning för eventuell menbedömning enligt ovan inleds.

I de fall nyckelansvarig har bedömt att en nyckel *inte är röjd* meddelas den som gjort anmälan (samt övriga som tagit del av den ursprungliga anmälan) att nyckeln inte är röjd. Inga ytterligare åtgärder behöver vidtas.

Nyckelansvarig ansvarar för att Högkvarteret (TSA) fortlöpande orienteras om inträffade nyckelincidenter samt vilka åtgärder som vidtagits.

Nyckelansvar vid övningar

Nyckelansvarig vid övningsanordnande myndighet/enhet skall i övningsorder eller motsvarande meddela tilldelning av nyckelserier TIFÖ (tillfälliga övningsnycklar) för genomförande av övning, samt särskilda förutsättningar för nyckelseriers användande under övningens genomförande.

I övningsorder eller motsvarande skall framgå vem som är nyckelansvarig för varje nyckelserie samt vem som ansvarar för/tar emot anmälan om nyckelincident. Nyckelansvarig myndighet framgår normalt av kryptonyckelns seriebeteckning.

Nyckelansvar vid användning av TIFÖ-nycklar åvilar övningsanordnande myndighet/enhet oavsett vad som framgår av nyckelns seriebeteckning. Dock skall alltid ordinarie nyckelansvarig orienteras om övningen och användning av aktuell nyckelserie.

Beställning/avbeställning sker enligt fastställd rutin. För de signalskyddschefer som har tillgång till IS UNDSÄK *skall* beställning/avbeställning göras i redovisningssystemet för kryptonycklar (IS UNDSÄK TSA).

Ordinarie nycklar

Följande anvisningar gäller i normalfallet, dvs vid mindre övningar eller då signalskyddet speciellt inte avses övas.

- Vid övningar med fredsorganisationens resurser skall normalt ordinarie nyckelserier för fred-/beredskap (F/B-nycklar) nyttjas.
- Om befintlig nyckeltilldelning ej täcker behovet av kryptonycklar vid övning krävs en tilläggsbeställning/fler exemplar av nycklar.
- En förutsättning för att nycklar i ordinarie F/B-nyckelserie skall kunna tilläggsbeställas och även användas i övningssammanhang är att nyckelansvarig myndighet har tecknat ”överex”-abonnemang avseende nyckelserien.

Tillfälliga övningsnycklar

TIFÖ-nycklar används vid större övningar eller då signalskyddet speciellt skall övas.

Beteckningen på en TIFÖ-nyckelserie skall överensstämma med märkningen av motsvarande ordinarie nyckelserie med det avslutande tillägget TIFÖ (eller förkortat TI) som tilläggsinformation.

Den som är utsedd att vara nyckelansvarig har uppgiften att fastställa beteckning på nyckelserie, fastställa och meddela tilldelning, samt driftsätta TIFÖ-nycklar inför övning.

I följande fall kan behov av att nyttja TIFÖ-nycklar uppstå.

- Vid försvarsmaktsövning eller övning inom det civila försvaret av motsvarande omfattning.
- Då ordinarie nycklar inte räcker/inte kan tilläggsbeställas till övning.
- Under särskilda övningsförutsättningar.
- Då signalskyddstjänsten särskilt skall övas, t ex avseende incidenter och nyckelbyten.

Samråd med Högkvarteret (TSA) bör ske inför beställning av TIFÖ-nycklar.

TIFÖ-nycklars giltighet kan hanteras på två olika sätt. Nyckelansvarig har uppgiften att fastställa om nyckelserie skall bestå av daterade nycklar eller om nycklarna endast skall innehålla lottningsnummer (LO-NR).

Om det i samband med övning inträffar en nyckelincident eller annan händelse som är ett hot mot signalskyddet, är det nyckelsansvarig vid den övningsanordnande myndigheten/enheten som ansvarar för att ärendet handläggs. Vidare anvisningar finns i avsnitt 6.3.13 ”Nyckelincident”. Det är av stor vikt att utbildning och information om användningen av signalskydd vid övningar delges berörda för att upprätthålla ett fullgott skydd och undvika incidenter.

6.4 Nyckelinjektor

Nyckelinjektor är en utrustning försedd med elektroniskt minne för säker lagring, transport och inläsning av kryptonycklar.

För att en nyckelinjektor skall ge avsedd effekt vad avser skydd och säkerhet vid lagring, transport och inläsning av nycklar måste den hanteras och förvaras enligt reglerna för signalskyddsmateriel. Se avsnitt 6.6 ”Signalskyddsmateriel.

6.4.1 PIN för nyckelinjektor

För att säkerställa att obehörig inte får tillgång till de kryptonycklar som lagrats, måste i vissa typer av nyckelinjektorer en engångs-PIN anges innan nyckelutläsningen kan påbörjas. Varje engångs-PIN hanteras som hemlig uppgift intill dess att den används.

6.4.2 Blankett för engångs-PIN

Blanketterna produceras vid Högkvarteret (TSA) i block om normalt femtio exemplar. Efter särskilt beslut kan produktionen förläggas till annan myndighet/enhet eller förband. Vid sådan produktion måste utrustning och metoder enligt Högkvarteret (TSA) bestämmande användas respektive tillämpas.

Varje blankett hanteras som hemlig handling och innehåller normalt åtta koder. För att kunna skilja på blanketterna i ett block är varje blankett märkt med ett löpnummer.

Förpackning och distribution

Vid förpackning och distribution gäller samma regler som för kryptonycklar enligt avsnitt 6.3.7 ”Förpackning och distribution”.

Delgivning

Signalskyddschef ansvarar för delgivning av blanketter för engångs-PIN inom eget ansvarsområde. För att undvika att samma PIN delges nyckelinläsare mer än en gång överkorsas delgiven PIN. Övriga regler för delgivning framgår av instruktion för respektive nyckelinjektor.

Hantering och förvaring

För att en nyckelinjektor som kräver PIN före utläsning av kryptonyckel, skall ge avsett skydd vid lagring, transport och inläsning av nycklar, krävs det att blanketterna hanteras och förvaras på ett sådant sätt att obehörig åtkomst förhindras. Blanketterna förvaras enligt samma regler som gäller för kryptonycklar enligt avsnitt 6.3.10 ”Hantering och förvaring”.

Förstöring

När alla engångs-PIN på en blankett är förbrukade eller när blanketten inte längre behövs för tjänsten skall den förstöras.

Röjd PIN

Om obehörig har haft möjlighet att ta del av en PIN kan denna vara röjd. Röjd PIN skall förstöras så att den inte av misstag delges för användning.

6.5 Nyckelserver

Nyckelserver är en utrustning med uppgift att elektroniskt säkerställa generering, administration och distribution av kryptonycklar vid kryptering mellan kryptoutrustningar i nät och mellan nät, t ex mellan GSM-kryptotelefoner eller VPN-kryptoapparater.

Nyckelserver med inlästa nycklar eller annan hemlig information klassificeras som hemlig signalskyddsmateriel. Plomberad nyckelserver utan inlästa nycklar och där minnesenhet med hemlig information är demonterad klassificeras som signalskyddsmateriel utan inläst kryptonyckel. Se avsnitt 6.6.6 ”Placering och förvaring”.

Ytterligare detaljerade regler för placering och förvaring av signalskyddsmateriel framgår av avsnitt 6.6.6 ”Placering och förvaring”.

I ett system med nyckelserver ingår normalt två typer av nycklar, *grundnyckel* och *sessionsnyckel*.

Grundnyckeln som endast finns i två exemplar läses in i nyckelserver och i kryptoutrustning. Den används för att kryptera kommunikationen mellan kryptoutrustning och nyckelserver. Sessionsnyckeln genereras i nyckelservern och distribueras elektroniskt. Denna nyckel är unik för varje kombination av sändare – mottagare.

6.5.1 Nyckelhantering

En nyckelserver förser två kryptoutrustningar som skall kommunicera med varandra med en gemensam nyckel för varje meddelande (session), under en viss tidsperiod eller för en viss mängd data. Denna nyckel benämns sessionsnyckel och används för att kryptera all information som utväxlas.

Säkerheten i systemet bygger på att varje kryptoutrustning har en grundnyckel som endast finns i utrustningen och i nyckelservern. Grundnyckeln används för att skydda de sessionsnycklar som nyckelservern distribuerar till kryptoutrustningarna.

Om inte annat framgår av instruktion för respektive system, gäller samma regler för grundnycklar avseende hantering, förvaring m m, som för övriga kryptonycklar enligt avsnitt 6.3 ”Kryptonycklar”.

Produktion

Grundnycklar produceras vid Högkvarteret (TSA-Lovön), i två exemplar av varje lottning. För att underlätta och förenkla distributionen kan, efter särskilt beslut, produktionen förläggas till annat ställe i an-

slutning till eller i den aktuella nyckelservern. Sessionsnycklar produceras normalt elektroniskt i en nyckelserver.

Distribution

Grundnycklar distribueras i två exemplar av varje lottning för senare inläsning i aktivt kort och nyckelserver. Distributionen sker enligt samma regler som gäller för övriga kryptonycklar. Om grundnyckel avsedd för nyckelserver distribueras på datamedia, krypteras informationen med en särskild kryptonyckel en s k transportnyckel. Transportnyckel får inte försändas tillsammans med de kryptonycklar den avser skydda.

Sessionsnycklar distribueras elektroniskt i krypterad form från nyckelserver till kryptoutrustningarna. Sessionsnycklars generering, administration och distribution i ett nyckelserversystem regleras i respektive systems instruktion.

Delgivning

Signalskyddschef ansvarar för att exemplar nr 1 av grundnyckeln läses in på det aktiva kort som skall nyttjas i kryptoutrustningen. Uppgift om var exemplar nr 1 skall nyttjas delges den som är ansvarig för respektive nyckelserver. Detta för att exemplar nr 2 av grundnyckeln ska kunna bindas till rätt kryptoutrustning/person i nyckelservern.

6.6 Signalskyddsmateriel

Till signalskyddsmateriel räknas kryptoapparat, komponent eller utrustning som innehåller kryptomodul eller krypteringsfunktion samt annan signalskyddsspecifik materiel eller signalskyddsspecifik programvara som används eller avses användas i ett signalskyddssystem.

Den signalskyddsmateriel som används inom totalförsvaret är normalt inte hemlig då det inte finns hemliga eller sekretessbelagda kryptonycklar lagrade i utrustningen. Sådan signalskyddsmateriel skall hanteras så att *manipulation* och *tillgrepp* av materielen förhindras.

För signalskyddsutrustning med inlästa och lagrade hemliga kryptonycklar, se avsnitt 6.6.6 ”Placering och förvaring”.

Signalskyddsmateriel, utom signalskyddsspecifik programvara, skall vara förseglad, med plombering eller lås, så att den som hanterar materielen kan konstatera om någon har försökt manipulera den.

Har signalskyddsmateriel eller försegling av sådan materiel utsatts för åverkan skall materielen omedelbart tas ur drift. Materielen skall hanteras på samma sätt som föreskrivs i 30 § i denna författning i fråga om hemlig signalskyddsmateriel.

Anmälan om åverkan skall omedelbart göras till signalskyddschefen och myndighetens säkerhetsskyddschef samt till Högkvarteret.

29 § FFS 2005:2

Det är varje användares *skyldighet* att regelbundet kontrollera materielens plomberingar.

För att få föra ut signalskyddsmateriel utanför svenskt territorium krävs godkännande av Högkvarteret.

28 § FFS 2005:2

Se även avsnitt 9 ”Signalskydd vid internationell verksamhet”.

6.6.1 Rutiner vid upphandling och utveckling

Upphandling för utveckling av signalskyddsmateriel sker normalt av FMV. Underlag för utveckling i form av målsättning för gemensamma signalskyddssystem lämnas av Högkvarteret (TSA). Underlag för funktionsspecifika signalskyddssystem lämnas, efter samråd med Högkvarteret (TSA), av den som har givit uppdraget om utveckling.

En myndighet som utvecklar eller låter utveckla signalskyddsmateriel som är avsedd att ingå i ett system med kryptografiska funktioner för signalskyddsgrad SG TS, SG S eller SG C eller för trafikskydd, skall se till att

1. *materielen konstrueras så att den inte avger röjande signaler (RÖS),*
2. *kryptoalgoritmer och beskrivningar av kryptoalgoritmer inte kommer till obehörigs kännedom,*
3. *kryptoalgoritmer i form av programvara hanteras i fristående datorer och i RÖS-godkänd miljö,*
4. *den som på myndighetens uppdrag erhåller eller utvecklar kryptoalgoritm för användning i ett sådant system förbinder sig att inte utnyttja kryptoalgoritmen, eller del av denna, i annat sammanhang utan skriftligt godkännande av Försvarsmakten, och*
5. *den som avses i punkten 4 förbinder sig att låta myndigheten nyttja kryptoalgoritmen, och dess källkod, för att kontrollera att den fungerar på önskat sätt och att kunna utveckla kryptoalgoritmen på det sätt signalskyddet kräver.*

26 § FFS 2005:2

En myndighet som upphandlar signalskyddsmateriel, eller programvara för sådan materiel, som har avgörande betydelse för att den totala säkerheten i systemet upprätthålls skall se till att leverantören genom avtal förbinder sig att följa regler för hantering och förvaring av signalskyddsmateriel.

27 § FFS 2005:2

6.6.2 Rutiner vid anskaffning och fördelning

Anskaffning av signalskyddsmateriel för totalförsvarets myndigheter/enheter sker normalt av FMV.

Underlag för anskaffning avseende Försvarsmakten lämnas av Högkvarteret. Underlag för civila myndigheter sammanhålls och lämnas av KBM utom för de myndigheter/enheter som själva lämnar underlag. Samtliga underlag skall lämnas till FMV efter samråd med Högkvarteret (TSA).

FMV ansvarar för beställningen hos industrin. Beställningen innehåller bl a en avtalad leveransplan som talar om i vilken takt materielen kommer att levereras till centralt förråd. Leveransplan med uppgift om när materielen kommer att levereras till centralt förråd, samt information om beställare och antal, skall tillsändas Högkvarteret (TSA).

Efter samråd med berörda fastställer Högkvarteret (TSA) en preliminär huvudfördelningsplan med leveransplanen som grund. Denna reglerar fördelningen till berörda myndigheter av levererad materiel per leveranstillfälle. Planen tillsänds berörda myndigheter samt det centrala förrådet.

När leverantören anmäler till FMV att materielen är klar för leverans utfärdar FMV, efter godkännande, leveranscertifikat för leveransomgången. En bekräftelse i form av en kopia av leveranscertifikatet sänds till Högkvarteret (TSA) som meddelar det centrala förrådet.

När materielen anlänt till det centrala förrådet meddelas FMV och Högkvarteret (TSA). Högkvarteret (TSA) ansvarar för fastställande och utgivning av slutlig huvudfördelningsplan för leveransomgången till berörda myndigheter, som i sin tur upprättar fördelningsplan för vidare fördelning av materielen.

För fördelning av signalskyddsmateriel i form av programvara tillämpas särskilda rutiner som normalt framgår av respektive godkännandeskrivelse.

Ansvar för fördelning av materiel

Försvarsmakten

Högkvarteret fördelar materiel ingående i gemensamma signalskyddssystem och säkra kryptografiska funktioner till Försvarsmaktens förband, staber och skolor, samt materiel ingående i funktionsspecifika system till de organisationsenheter som skall utrustas med systemet.

Försvarsmakten närstående myndigheter

Försvarets materielverk, Försvarets radioanstalt, Försvarshögskolan, Totalförsvarets forskningsinstitut, Totalförsvarets Pliktverk och Fortifikationsverket fördelar materiel ingående i gemensamma signalskyddssystem och säkra kryptografiska funktioner till respektive myndighets organisationsenheter, vad avser Försvarets materielverk även till försvarsindustrin.

Krisberedskapsmyndigheten (KBM)

KBM fördelar materiel ingående i gemensamma signalskyddssystem och säkra kryptografiska funktioner till riksdagen, regeringskansliet samt till övriga civila myndigheter/enheter *utom* till de myndigheter/enheter ovan som själva fördelar materielen. KBM ansvarar även för fördelning av materiel och säkra kryptografiska funktioner till samhällsviktiga företag.

Respektive myndighet

Materiel som ingår i en myndighets/enhets funktionsspecifika system fördelas av respektive myndighet till de organisationsenheter som skall utrustas med systemet.

6.6.3 Rutiner vid begäran om materiel utöver grundtilldelning

Vid anskaffning av signalskyddsmateriel anskaffas i regel endast den mängd materiel som det fanns ett behov av vid anskaffningstillfället. Någon extra materiel för ytterligare tilldelning eller utlåning anskaffas normalt inte. Det innebär att då nya behov uppkommer och en till-

läggsbeställning inte kan göras måste en omfördelning av anskaffad materiel ske.

Detta innebär att projekt eller motsvarande, själva måste säkerställa att behov av signalskyddsmateriel vid framtagande av nya telekommunikations- och IT-system anmäls till den som ansvarar för anskaffning (enligt avsnitt 4.1 ”Ansvar och uppgifter”). Detta gäller även vid införande av nya tekniska lösningar i befintliga system.

Vid organisationsförändringar kan dock viss materiel frigöras för fördelning eller utlåning. Denna materiel förrådsställs centralt och förvaltas för Försvarsmaktens del av Högkvarteret och för civila myndigheter av KBM.

Behovsframställan

Försvarsmaktens förband, staber och skolor anmäler skriftligt sitt behov av materiel till Högkvarteret. Behov av materiel för civila myndigheter anmäls till KBM.

Försvarsmakten närstående myndigheter kan efter begäran till Högkvarteret beviljas lån av materiel för tillfälliga behov.

För att en begäran om behov av materiel skall kunna hanteras på ett effektivt och rationellt sätt bör följande uppgifter ingå i begäran.

- Om behovet avser lån eller tilldelning.
- En beskrivning av varför materielen erfordras.
- Vid lån för prov och försök bör hänvisning till uppdrag eller motsvarande även framgå av begäran.
- I förekommande fall, namn på ansvarig för prov och försök.
- Förrådsbenämning, förrådsbeteckning och antal utrustningar motsv.
- Under vilken tid materielen erfordras.
- Leveransadress och namn på kontaktperson.
- Faktureringsadress för kostnader som kan uppstå.
- Underskrift av behörig befattningshavare samt sändlista.

Behov av, samt begäran om materiel, bör handläggas av signalskyddschefen eller av signalskyddschefen särskilt utsedd person vid den begärande myndigheten/enheten. Handläggs ärendet av någon annan skall behovsframställan tillställas myndighetens/enhetens signalskyddschef.

6.6.4 Förpackning och distribution

Före försändning av signalskyddsmateriel skall utrustningen nollställas och samtliga kryptonycklar raderas ur utrustningens minne.

Innehållet i försändelsen aviseras som sambandsmateriel. Under grundberedskap meddelar avsändaren i skrivelse till mottagaren materielens art, antal, individnummer, avsändningsdatum, försändningssätt och adress. I förekommande fall anges att utrustningen inte är nollställd och/eller plomberad samt orsaken härtill.

Den som tar emot en försändelse med signalskyddsmateriel kontrollerar att emballage, låsanordningar samt plomberingar är oskadade. Mottagaren kontrollerar även att innehållet stämmer överens med uppgifterna på följesedel eller förhandsmeddelande om att distribution skall ske.

Mottagaren anmäler omedelbart till signalskyddschef när materiel har mottagits samt även till säkerhetsskyddschef då skada, som uppkommit under försändningen, konstaterats på materiel, plombering, låsanordning eller emballage. Signalskyddsmateriel med skadad eller bruten plombering eller låsanordning hanteras som hemlig signalskyddsmateriel.

Hemlig signalskyddsmateriel och signalskyddsmateriel som har utsatts för åverkan eller har bruten eller skadad försegling samt låsnycklar till signalskyddsmateriel och till transportbehållare som används för signalskyddsmateriel skall försändas i förseglat emballage och befordras med en distributör som har godkänts av myndigheten. Låsnycklarna skall försändas i en separat försändelse.

Emballaget skall vara så beskaffat att det inte går att få information om materielen i emballaget utan att bryta det. Förseglingen skall vara sådan att det går att se om någon har brutit emballaget.

Signalskyddsmateriel som inte är hemlig skall försändas på ett sådant sätt att manipulation och tillgrepp av materielen förhindras.

30 § FFS 2005:2

Rekommendationer vid försändning

Vid försändning av signalskyddsmateriel inrikes bör Posten eller FMLOG Fjärrgods nyttjas. Då Posten nyttjas sänds signalskyddsmateriel med ”Posten värde”. Vid nyttjande av FMLOG Fjärrgods får Transportbehållare 601 eller 602 användas som transportemballage men medför inget extra säkerhetsskydd. Civil myndighet/enhet kan beställa transportbehållare från närliggande förband.

Vid försändning av signalskyddsmateriel utrikes gäller särskilda bestämmelser enligt avsnitt 9.2 ”Bestämmelser för utförsel, införsel samt återförsel”.

Låsnycklar till transportbehållare samt eventuella låsnycklar till signalskyddsutrustning sänds separat med ”Posten värde” eller motsvarande.

Signalskyddsmateriel kan försändas på annat sätt eller medföras av betrodd person om det kan ske på ett sådant sätt att materielen är under ständig uppsikt och att obehörig inte kan komma åt materielen.

6.6.5 Redovisning

Varje myndighet som har signalskyddsmateriel skall förteckna materielen i ett register med angivande av individnummer. Registret skall ständigt hållas aktuellt. Om myndigheten består av flera enheter gäller detta varje enhet.

31 § första stycket FFS 2005:2

Utöver individnummer redovisas förrådsbenämning, förrådsbeteckning och myndighet/enhet eller förband som tilldelats materielen. Vid myndighet/enhet redovisas även var materielen är förvarad eller placerad. Detta skall framgå av myndighetens/enhetens signalskyddsinstruktion eller motsvarande. Registret över signalskyddsmaterielen skall innehålla aktuella och uppdaterade uppgifter, särskilt avseende materielens individnummer och materielens placering/förvaring, t ex aktuellt rumsnummer, säkerhetsskåpsnummer eller motsvarande. Då utbytesapparat erhålls vid reparation eller underhåll måste individnummer i redovisningssystemet ändras genom redovisande myndighetens/enhetens försorg. Som stöd för redovisningen används inom Försvarsmakten redovisningssystemet LIFT.

Signalskyddsmaterielen skall inventeras varje år samt vid byte av befattningshavare som ansvarar för sådan materiel. Inventeringen skall förrättas av signalskyddschefen eller en av myndigheten särskilt utsedd befattningshavare.

31 § andra stycket FFS 2005:2

Genomförd inventering skall efter anmodan rapporteras till Högkvarteret (TSA). Rapporten skall omfatta uppgifter om myndighet/enhet, ansvarig, förrådsbenämning, förrådsbeteckning samt individnummer över myndighetens/enhetens signalskyddsmateriel.

Större sammanställningar av antalet utrustningar får endast framgå av sekretessbelagd handling. Se bilaga 2 om sekretessbedömning för ytterligare information.

Beteckning av materiel

Signalskyddsmateriel indelas efter huvudsakligt användningsområde och betecknas med tre siffror enligt tabellen nedan.

Tabell 13. Beteckningar och användningsområden för signalskyddsmateriel

Beteckning	Huvudsaklig användning
100 – 199	Förbindelsekryptering av låghastighetsdata
200 – 299	Lokalkryptering, t ex hårddiskkrypto
300 – 399	Lokalkryptering, små informationsmängder
400 – 499	Förbindelsekryptering telefax
500 – 599	Förbindelsekryptering höghastighetsdata
600 – 699	Kryptering för speciella ändamål
700 – 799	Förbindelsekryptering av tal för operativt bruk
800 – 899	Förbindelsekryptering av tal för taktiskt bruk
900 – 999	Förbindelsekryptering av data

Signalskyddsmateriel betecknas och märks även med ett materielnummer s k M-nr (t ex M3858-760010) samt ett unikt individnummer för varje utrustning.

6.6.6 Placering och förvaring

Hemlig signalskyddsmateriel samt signalskyddsmateriel, aktiva kort och annan liknande materiel, med inläst kryptonyckel för signalskyddsgrad SG TS, SG S, SG C eller kryptonyckel som är märkt med beteckningen trafikskydd, skall stå under ständig uppsikt eller förvaras i ett utrymme som uppfyller lägst kraven för säkerhetsskåp enligt Standardiseringskommissionens normer (SIS), Svensk Standard (SS) 3492.

Övrig signalskyddsmateriel skall placeras och förvaras så att manipulation och tillgrepp av materielen förhindras.

32 § FFS 2005:2

Vid val av förvaringsutrymme för övrig signalskyddsmateriel (enligt definitionen ovan) måste hänsyn tas till den allmänna skyddsnivån; skalskyddet på förvaringsutrymmet, dess geografiska läge (bevakat område eller ensligt belägen plats) och tillträdesskyddet till den lokal, där förvaringsutrymmet är placerat. I vissa fall kan det vara nödvändigt att förse utrymmet med larmanordning.

Underhåll och reparation

Vid behov av underhåll eller reparation av signalskyddsmateriel skall civila myndigheter vända sig till KBM. Försvarsmaktens förband, skolor och centra skall vända sig till central kryptoverkstad. För detaljerad information se respektive systems godkännandeskrivelse eller instruktion.

6.6.7 Materielincident

Förlust eller misstanke om manipulation av signalskyddsmateriel skall omedelbart anmälas till signalskyddschefen, myndighetens säkerhetsskyddschef och till den som anskaffat eller tilldelat materielen samt till Högkvarteret.

34 § FFS 2005:2

Har signalskyddsmateriel eller försegling av sådan materiel utsatts för åverkan skall materielen omedelbart tas ur drift. Materielen skall hanteras på samma sätt som föreskrivs i 30 § i denna författning i fråga om hemlig signalskyddsmateriel.

Anmälan om åverkan skall omedelbart göras till signalskyddschefen och myndighetens säkerhetsskyddschef samt till Högkvarteret.

29 § andra och tredje stycket FFS 2005:2

Med ”Högkvarteret” ovan menas att anmälan skall ske till Högkvarteret (TSA).

Exempel på innehåll i anmälan om materielincident:

- Tidpunkt samt under vilka omständigheter misstanke om manipulation/förlust/funktionsfel har skett.
- Förrådsbenämning (kryapp XXX).
- Förrådsbeteckning (M XXX-XXX).
- Individnummer.
- Vid vilken enhet incidenten har skett.
- Vidtagna åtgärder.
- Telefonnummer (krypto) till signalskyddschef eller motsvarande.

6.6.8 Utlåning och överlåtelse

En myndighet får inte låna ut signalskyddsmateriel till någon som inte omfattas av föreskrifterna i denna författning, om inte överenskommelse har träffats mellan myndigheten och den som mottar materielen om att tillämpa innehållet i denna författning.

35 § FFS 2005:2

Överlåtelse av signalskyddsmateriel får endast ske till en annan statlig myndighet.

33 § FFS 2005:2

6.6.9 Avveckling och förstöring

Signalskyddsmateriel får endast avvecklas och förstöras med en metod som är godkänd av Högkvarteret.

36 § FFS 2005:2

Högkvarteret beslutar om avveckling av signalskyddsmateriel ingående i gemensamma system samt i funktionsspecifika system för Försvarsmakten. Efter beslut om avveckling ger Högkvarteret uppdrag till FMV att genomföra avvecklingen. FMV reglerar i särskild avvecklingsskrivelse hur avvecklingen skall genomföras. Materiel ingående i övriga funktionsspecifika system avvecklas av respektive ansvarig myndighet i samråd med Högkvarteret (TSA).

Enskild myndighet/enhet får inte på eget initiativ avyttra, avveckla, avregistrera eller förstöra signalskyddsmateriel, om inte annat framgår av respektive systemgodkännande.

När en myndighet/enhet skall avveckla sin signalskyddsmateriel och/eller signalskyddsverksamhet skall samtlig signalskyddsmateriel återlämnas. Försvarsmaktens enheter och förband återlämnar materielen till centralt militärt förråd och civila myndigheter återlämnar materielen till KBM.

Anvisningar för begränsad respektive total förstöring, när omedelbar fara föreligger för att kryptonyckel, signalskyddshandling, signalskyddsmateriel eller förbandsregister skall falla i motståndarens händer, framgår av bilaga 6.

6.7 Instruktioner

Högkvarteret fastställer instruktioner för hantering av gemensamma signalskyddssystem samt instruktioner för funktionsspecifika system avsedda för Försvarsmakten. Instruktioner för övriga funktionsspecifika system, fastställs av den myndighet som utvecklat systemet.

> *Varje myndighet som har anskaffat eller tilldelats ett signalskyddssystem skall följa de instruktioner som Högkvarteret meddelar i fråga om användningen av systemet.*
>
> 6 § FFS 2005:2

Fastställda och utgivna bestämmelser för äldre system gäller intill dess att de upphävs. Bestämmelserna skall intill dess de upphävs betraktas som instruktioner och därmed följas enligt ovanstående föreskrift.

Instruktion för signalskyddssystem eller handbok för telekommunikations- och IT-system i vilka krypteringsfunktion ingår fastställs i samråd med Högkvarteret (TSA).

6.7.1 Utformning och omfattning

Instruktioner för gemensamma system samt instruktioner för funktionsspecifika system avsedda för Försvarsmakten utformas enligt Försvarsmaktens grafiska profil.

Instruktion eller handbok som beskriver hantering och handhavande av signalskyddssystem bör inledas med ett avsnitt som ger en kort beskrivning av signalskyddet i systemet samt bestämmelser för signalskyddsmateriel och kryptonycklar, såsom förvaring, försändning, förstöring samt åtgärder vid signalskyddsincident. I avsnittet bör även framgå bestämmelser för utbildning på det aktuella systemet.

Högkvarteret (TSA) kan bistå med råd och anvisningar vid utformning av publikationer enligt ovan.

Kapitel 7
Aktiva kort, certifikat och kortterminaler

Detta kapitel beskriver och reglerar övergripande användning och hantering av aktiva kort, certifikat och kortterminaler. För utförlig beskrivning se särskild instruktion I TST AKT.

7.1 Aktiva kort

Aktiva kort har tagits fram av Försvarsmakten för användning inom totalförsvaret i olika system som kräver säker identifiering av användare vid behörighetskontroll (autentisering). Vissa aktiva kort (TAK och TEID) är dessutom avsedda att användas för signering av information (digital signatur) samt som bärare av data, främst kryptonycklar. Korten kan även användas för kryptering.

Ett aktivt kort innehåller en dator i form av ett mikrochip med processor och minne för att lagra program och data. Via kontaktytorna på kortet förses chipet med ström och kommunikation med omvärlden blir möjlig när kortet förs in i en kortterminal eller kortläsare. Chipet innehåller även ett operativsystem som är utvecklat för att garantera

säkerheten för de uppgifter som lagras på chipet. Operativsystemet kräver koder (PIN) för att kunna användas vid autentisering, skapande av digital signatur och in/utläsning av kryptonycklar.

Aktiva kort indelas i

TAK, Totalförsvarets Aktiva Kort, avsett

– för identifiering av användare,

– för signering av information, eller

– som bärare av kryptonycklar.

37 § första stycket FFS 2005:2

Sedan fastställandet av FFS 2005:2 har vissa fysiska egenskaper och kapaciteten hos TAK förbättrats. Förutom att vara bärare av kryptonycklar kan TAK även vara bärare av övriga data.

TEID, Totalförsvarets Elektroniska ID-kort, avsett

– för identifiering av användare,

– för signering av information,

– som bärare av data, eller

– som bärare av kryptonycklar avsedda för signalskyddsgrad SG R.

NBK, Totalförsvarets Nyckelbärarkort, avsett

– som bärare av data eller kryptonycklar.

37 § andra och tredje stycket FFS 2005:2

Utöver ovan aktiva kort finns även databärarkort (DBK) avsett för lagring av data samt nyckelbärarkort av äldre typ (TAK/NBK) som används för att hantera kryptonycklar för äldre system.

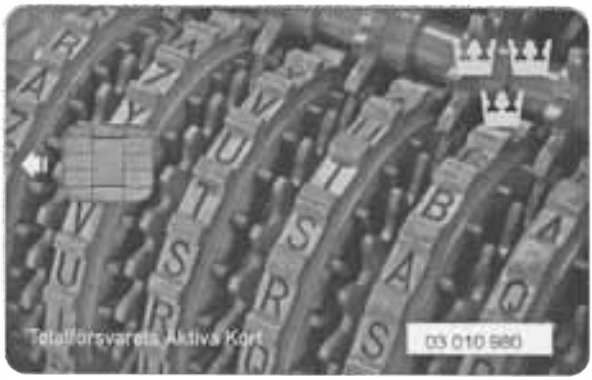
Korten tillverkas i kreditkortsformat med unika serienummer om åtta siffror. Baksidan är vit med påskrift om hur upphittat kort skall han-

teras. För att särskilja olika typer av kort har de försetts med olika färg och tryck på framsidan. NBK och TEID finns även i SIM-kortsformat.

TAK och TEID är normalt personliga och är därmed inte kopplade till något specifikt system eller någon specifik arbetsplats utan kan nyttjas av användaren i flera olika system/platser.

Förutsättningen för att de aktiva korten skall kunna nyttjas i olika system är dock att respektive system nyttjar särskild programvara som stödjer användning av aktiva kort. Om sådan programvara avser skydda sekretessbelagd information skall den vara godkänd av Högkvarteret (TSA).

7.1.1 Beskrivning Totalförsvarets aktiva kort (TAK)



Totalförsvarets Aktiva Kort (TAK).

TAK är ett personligt kort knutet till en viss person eller i undantagsfall en roll. Kort levereras försedda med användarens privata RSA-nycklar (en för signering och en för autentisering/kryptering) och certifikat samt certifikatutgivarens certifikat. TAK är avsett att användas i system som omfattas av sekretess.

TAK och NBK får endast användas i kortterminaler eller kortläsare som har godkänts av Högkvarteret och endast tillsammans med programvaror som är godkända för TAK respektive NBK.

38 § FFS 2005:2

Till godkänd kortterminal räknas KT2 eller KT ADM. Godkänd kortläsare är även sådan kortläsare som finns i försvarsmaktsgodkänd kryptoutrustning.

Så länge användaren har en tjänst inom en myndighet kan samma kort användas till flera olika system, då certifikaten inte innehåller någon organisationsspecifik information annat än myndighet.

Varje kort som försetts med certifikat är unikt, och är alltid knutet till en bestämd person eller roll. Kortets certifikat kan ha olika giltighetstid beroende på kortets användningsområde m m. Det normala är dock en giltighetstid på max tre år. Därefter kan kortet bytas ut eller förses med nytt certifikat. Behov av TAK eller certifikat anmäls till respektive myndighets/enhets kortadministratör. Exempel på kvitto för TAK se bilaga 9.

7.1.2 Beskrivning Nyckelbärarkort (NBK)

Totalförsvarets Nyckelbärarkort (NBK).

Nyckelbärarkort är inte knutna till en viss person eller roll utan endast avsedda som nyckelmedia för lagring av data i form av kryptonycklar. Dessa kort återfinns i två varianter, dels ett vanligt NBK i kontokortsformat (kallas NBK), dels ett mindre NBK i SIM-kortsstorlek (kallas NBK-SIM). Eftersom funktionaliteten är lika för de olika formaten på korten kommer för tydlighetens skull i texten endast refereras till NBK. NBK kan lagra en större mängd kryptonycklar.

> *TAK och NBK får endast användas i kortterminaler eller kortläsare som har godkänts av Högkvarteret och endast tillsammans med programvaror som är godkända för TAK respektive NBK.*
>
> 38 § FFS 2005:2

Till godkänd kortterminal räknas KT2 eller KT ADM. Godkänd kortläsare är även sådan kortläsare som finns i försvarsmaktsgodkänd kryptoutrustning.

7.1.3 Beskrivning TAK/NBK

Bild 11 Äldre modell av Totalförsvarets Nyckelbärarkort (TAK/NBK).

TAK/NBK är ett nyckelbärarkort av den äldre generationens aktiva kort. Kortet är inte knutet till en viss person eller roll utan endast avsett som nyckelmedia för lagring av data i form av kryptonycklar.

Observera att TAK/NBK i huvudsak skall användas till kryptotelefon 710 till dess att annat meddelas. För alla andra system som kräver nyckelbärarkort skall den nya versionen, NBK, användas.

7.1.4 Beskrivning Totalförsvarets elektroniska ID-kort (TEID)

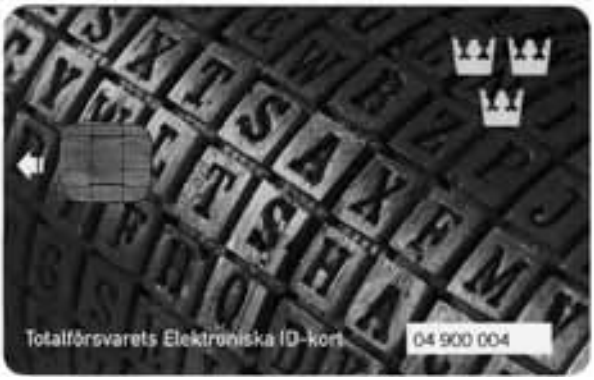


Bild 12 Totalförsvarets Elektroniska ID-kort (TEID).

TEID är ett personligt kort knutet till en viss person eller i undantagsfall en roll. Kort levereras försedda med användarens privata RSA-nycklar (en för signering och en för autentisering/kryptering) och certifikat samt certifikatutgivarens certifikat. TEID återfinns i två varianter, dels ett vanligt TEID i kontokortsformat (kallas TEID), dels ett mindre TEID i SIM-kortsstorlek (kallas TEID-SIM). Eftersom funktionaliteten är lika för de olika formaten på korten kommer för tydlighetens skull i texten endast refereras till TEID.

TEID är i första hand avsett för att användas i system som ej omfattas av sekretess, men kan efter godkännande av Högkvarteret (TSA) även användas i vissa system som omfattas av sekretess.

TEID är godkänt att använda i kommersiell kortläsare dvs det finns inget krav på att nyttja försvarsmaktsgodkänd läsare, för mer information se I TST AKT.

Så länge användaren har en tjänst inom en myndighet kan samma kort användas till flera olika system, då certifikaten inte innehåller någon organisationsspecifik information annat än myndighet.

Varje kort som försetts med certifikat är unikt, och är alltid knutet till en bestämd person eller roll. Kortets certifikat kan ha olika giltighetstid beroende på kortets användningsområde m m. Det normala är dock en giltighetstid på max fem år. Därefter kan kortet bytas ut eller förses med nytt certifikat. Behov av TEID eller certifikat anmäls till respektive kortadministratör. Exempel på kvitto för TEID se bilaga 9.

7.1.5 Beskrivning Databärarkort (DBK)

Databärarkort är inte knutna till en viss person eller roll utan endast avsedda för att lagra övriga data, t ex konfigurationsinställningar för kryptoapparater. Observera att kryptonycklar *inte* får lagras på DBK.

Kommersiella kortläsare får användas tillsammans med DBK, dvs inga krav föreligger på att nyttja försvarsmaktsgodkänd kortläsare.

7.2 Beskrivning mjuka certifikat

För servrar eller datorer med behov av att kunna utföra många autentiseringar eller signaturer per tidsenhet räcker inte kapaciteten hos ett aktivt kort till. För vissa servrar/datorer är det inte heller lätt att ansluta en kortterminal. För sådana fall används RSA-nyckelpar och certifikat levererade på en CD, i form av en fil skyddad med ett lösenord, som läses in i servern/datorn. Eftersom dessa certifikat levereras i form av mjukvara kallas de mjuka certifikat. System utan högre säkerhetskrav kan även nyttja mjuka certifikat. Mjuka certifikat återfinns i två varianter, användar- och servercertifikat. RSA-beräkningarna utförs av program i server eller dator.

Beroende på vad det mjuka certifikatet skall användas till kan CD:n vara märkt hemlig eller med signalskyddsgrad SG R.

7.3 Allmänt om koder (PIN och PUK) samt lösenord

Erforderlig PIN, PUK för att ta ett aktivt kort i bruk, alternativt lösenord för ett mjukt certifikat, produceras vid Högkvarteret (TSA). PIN, PUK eller lösenord anges på en datapost som produceras till kortet och som levereras direkt till användaren.

Vid utlämning av ett aktivt kort till en användare måste användaren låsa upp kortet med hjälp av den PUK som anges på dataposten. Användaren väljer samtidigt de PIN som skall användas.

PIN och PUK till det aktiva kortet samt lösenord för ett mjukt certifikat skall hanteras så att obehörig ej kan ta del av dessa och får endast delges till och vara känd av den person som har ansvaret för koderna.

7.4 Utgivning och personalisering

Högkvarteret (TSA) är ansvarig certifikatutgivare, CA, för TAK och TEID samt mjuka certifikat. CA är ansvarig för att TAK och TEID personaliseras (knyts till viss person eller roll) innan distribution sker till beställare inom totalförsvaret.

> *En myndighet som skall ge ut och knyta ett TAK och TEID till en viss person eller funktion (personalisering) får endast använda utrustning, programvara och metoder som har godkänts av Högkvarteret.*
>
> *I samband med personalisering får TAK och TEID endast hanteras i tillträdesbegränsat utrymme och så att obehöriga inte får insyn i verksamheten.*
>
> 41 § första och andra stycket FFS 2005:2

För att säkerställa att ingen obehörig skall kunna använda kortet innan det lämnas ut till användaren blockerar CA kortet för användning omedelbart efter genomförd personalisering.

CA publicerar utfärdade certifikat samt revokeringslistor (Certificate Revocation List, CRL) på en server som utgör underlag för katalogtjänst. En revokeringslista ger information om vilka certifikat som har revokerats, dvs har förklarats ogiltiga.

Det personaliserade kortet med tillhörande kvitton (se exempel bilaga 9) förpackas och försänds därefter till kortadministratören som ansvarar för utlämning av kortet till användaren. Dataposten skickas direkt till användaren.

7.5 Allmänt om beställning

Till varje TAK och TEID skall kvitto för aktivt kort upprättas i två exemplar. Ett kvittoexemplar skall efter kvittens av kortanvändaren återsändas till Högkvarteret. Det andra kvittoexemplaret skall förvaras av användaren.

39 § FFS 2005:2

Signalskyddschef eller kortadministratör skall ansvara för beställning, utlämning och uppföljning av aktiva kort.

Vid beställning och utlämning av aktiva kort skall den blivande användarens identitet kontrolleras.

40 § FFS 2005:2

Behov av aktiva kort eller mjuka certifikat anmäls till respektive myndighets/enhets kortadministratör, för detaljer se I TST AKT.

7.5.1 Allmänt om förpackning, distribution och utlämning

Före distribution från CA förpackas de aktiva korten i en sk kortförpackning. Sådan förpackning kan utgöras av vakuumförsluten påse tillverkad i ogenomskinligt plastlaminat och får endast innehålla ett kort.

Varje myndighet skall se till att erforderliga skyddsåtgärder vidtas vid försändning av aktiva kort.

Aktiva kort skall försändas i förseglat emballage. Emballaget skall vara så beskaffat att det inte går att ta del av innehållet utan att bryta emballaget. Förseglingen skall vara sådan att det går att se om någon har brutit emballaget.

Det förseglade emballaget skall innehålla ett förseglat innerkuvert som skall vara försett med påskrift att det innehåller aktivt kort och att det skall överlämnas obrutet till den som är signalskyddschef eller till den som myndigheten har bestämt.

42 § FFS 2005:2

Vissa rollkort, NBK samt TAK/NBK får dock förpackas med flera kort i en förpackning. På varje kortförpackning skall framgå inneliggande korts serie-/medianummer.

CD med mjukt certifikat förpackas tillsammans med kvitton i ett vadderat innerkuvert. Om CD:n är märkt hemlig eller SG R försluts detta med förseglingstejp. Mottagningsbevis bifogas. Det vadderade innerkuvertet förpackas i säkerhetskuvert (försändelse) tillsammans med följesedel. På innerkuvertet skall det klart och tydligt framgå att det skall överlämnas obrutet till kortadministratör och i förekommande fall att det innehåller CD märkt hemlig eller SG R.

Distribution av aktiva kort/mjuka certifikat med tillhörande handlingar skall dokumenteras, för detaljer se I TST AKT.

Högkvarteret (TSA) ansvarar för distribution av aktiva kort och mjuka certifikat, såväl under grundberedskap som efter höjd beredskap. Distributionen sker direkt till beställande myndighet/enhet, förband, stab eller skola.

Varje myndighet/enhet, förband, stab eller skola reglerar i signalskyddsinstruktion eller motsvarande hur försändelser med aktiva kort/mjuka certifikat, kvitton och datapost skall tas emot och återsändas.

7.5.2 Försändning

När aktiva kort och kvitton för aktiva kort försänds skall en följesedel bifogas. Av följesedeln skall framgå kortets och kvittots serienummer samt vem de är avsedda för. Följesedeln skall registreras vid mottagandet och sparas i minst tio år.

43 § FFS 2005:2

Ovanstående gäller även mjuka certifikat samt kvitton för dessa. Observera att NBK och DBK inte försänds med kvitton.

Vid försändning av aktiva kort och mjuka certifikat till utlandet tillämpas särskilda rutiner. Regler och rutiner fastställs av Högkvarteret (TSA).

7.5.3 Utlämning

När aktiva kort lämnas ut skall signalskyddschefen eller kortadministratören se till att kortet kvitteras av mottagaren.

44 § FFS 2005:2

Ovanstående gäller även mjuka certifikat på CD.

Det är av största vikt att signalskyddschefen eller kortadministratören kontrollerar användarens identitet före utlämnandet.

7.6 Allmänt om hantering och förvaring

Aktiva kort skall förvaras och hanteras på ett sådant sätt att obehörig hantering och tillgrepp förhindras.

45 § första stycket FFS 2005:2

För att uppnå åsyftad säkerhet vid användning av aktiva kort/mjuka certifikat i dess olika tillämpningar krävs att användaren ständigt har kontroll över sitt kort/CD och att PIN (personlig identifieringskod), PUK (personlig upplåsningskod) eller lösenord ej röjs för annan person. PIN, PUK eller lösenord skall hanteras så att obehörig ej kan ta del av koden. Byte av koder/lösenord behöver endast ske när misstanke om röjd sådan föreligger.

Aktiva kort som innehåller kryptonycklar för signalskyddsgrad SG TS, SG S eller SG C skall stå under ständig uppsikt eller förvaras i ett utrymme som uppfyller lägst kraven för säkerhetsskåp enligt Standardiseringskommissionens normer (SIS), Svensk Standard (SS) 3492.

45 § andra stycket FFS 2005:2

Ovanstående gäller även mjuka certifikat på CD märkt hemlig samt datapost.

Observera att även aktivt kort med kryptonyckel märkt med beteckningen trafikskydd skall stå under ständig uppsikt eller förvaras i ett utrymme som uppfyller lägst kraven för säkerhetsskåp enligt ovanstående standard. Se även 32 § FFS 2005:2 under avsnitt 6.6.6 ”Placering och förvaring”.

Aktiva kort som ej innehåller kryptonycklar för signalskyddsgrad SG TS, SG S eller SG C samt mjuka certifikat på CD märkt SG R skall förvaras så att obehörig hantering och tillgrepp förhindras.

Om obehörig haft tillgång till ett aktivt kort måste det återlämnas till myndighetens/enhetens kortadministratör som vidtar åtgärder enligt I TST AKT.

7.6.1 Allmänt om revokering

Revokering av certifikat innebär att certifikatet återkallas innan det upphört att gälla. Det är certifikatinnehavarens ansvar att, i första hand via kortadministratören och i andra hand direkt, begära revokering hos CA. När och hur revokering skall ske framgår av I TST AKT.

7.6.2 Allmänt om redovisning

> *Aktivt kort skall förtecknas i ett register. Av registret skall framgå kortets serienummer samt i förekommande fall certifikat. Om myndigheten består av flera enheter gäller detta varje enhet.*
>
> 41 § tredje stycket FFS 2005:2

Vid personalisering av TAK och TEID dokumenterar Högkvarteret (TSA) i ett centralt kortregister kortens serie-/medianummer samt certifikat. För NBK och TAK/NBK dokumenteras endast kortets serie-/medianummer och användningsområde.

Aktiva kort/mjuka certifikat redovisas mot den som distribuerat korten/mjuka certifikaten. Underlag för redovisning är följesedeln. För mer information om redovisning, se I TST AKT.

7.7 Allmänt om återlämning

7.7.1 Aktiva kort

Aktiva kort som har upphört att gälla, kort som inte längre behövs för tjänsten och/eller kort som skadats eller på annat sätt är felaktigt så att det inte kan användas på avsett vis, återlämnas till myndighetens/enhetens kortadministratör. Användaren måste innan kortet återlämnas radera inlästa kryptonycklar samt blockera sina koder. Information om blockerade koder se I TST AKT.

Kortadministratören skall bestyrka, med namnteckning, datum och klockslag, på användarens kvitto (gäller ej NBK och DBK) att aktivt kort är återlämnat. Certifikaten skall revokeras, om de inte har upphört att gälla. Det aktiva kortet skall återsändas till CA när certifikatet har upphört att gälla eller har revokerats.

7.7.2 Mjuka certifikat

CD märkt hemlig alternativt SG R innehållande mjuka certifikat, vilka har upphört att gälla, inte längre behövs för tjänsten och/eller är felaktiga återlämnas till myndighetens/enhetens kortadministratör.

Kortadministratören skall bestyrka, med namnteckning, datum och klockslag, på användarens kvitto att CD är återlämnad. Certifikaten skall revokeras, om de inte har upphört att gälla. CD märkt hemlig eller märkt SG R skall efter återlämning förstöras så att data ej kan återskapas, alternativt återsändas till CA när certifikat har upphört att gälla eller revokerats.

7.8 Allmänt om incident med aktivt kort eller mjukt certifikat

Den som har förlorat ett aktivt kort skall omedelbart anmäla förlusten till signalskyddschefen eller kortadministratören, till myndighetens säkerhetsskyddschef samt till Högkvarteret.

46 § FFS 2005:2

Ovanstående gäller även mjuka certifikat.

Förlust eller obehörig åtkomst till aktivt kort/mjukt certifikat eller koder/lösenord anmäls i första hand till lokal kortadministratör som ansvarar för att anmälan kommer vidare till Högkvarteret (TSA). Finns inte kortadministratören tillgänglig måste anmälan göras direkt till Högkvarteret (TSA). Den som förlorat ett aktivt kort eller mjukt certifikat måste även anmäla förlusten till respektive systemadministratör för de system där korten brukas.

I de fall där kryptonycklar finns inlästa på det förlorade kortet måste även anmälan om nyckelincident ske.

Exempel på innehåll i anmälan om incident för aktivt kort/certifikat/datapost/grundhandling.

- Tidpunkt samt under vilka omständigheter aktivt kort/certifikat/datapost/grundhandling kom bort.
- Kortets/CD:ns serie/medianummer.
- Datum och klockslag för förlustanmälan.
- Kortadministratörens namn, tjänstgöringsplats och telefonnummer.
- Typ/class av kort/certifikat.
- Innehavarens namn, personnummer, tjänstgöringsplats.
- Vidtagna åtgärder (revokering m m).

7.8 Kortterminaler

Bild 13 Kortterminal administration 9090 (KT ADM) och kortterminal 2 för användare (KT2).

För att ett aktivt kort skall bli användbart i ett system krävs, förutom en särskild programvara, en kortterminal eller kortläsare som utför kommunikationen mellan dator/motsvarande och kort. Kortterminalens knappsats används för att ange de koder som möjliggör kommunikation med kortet. Kortläsarfunktion kan finnas inbyggd i hårdvara som nyttjar aktiva kort, exempelvis dator, telefon eller inpasseringssystem. I sådan applikation används normalt hårdvarans knappsats för att ange PIN.

Kortterminalerna finns i två varianter, kortterminal administration 9090 (KT ADM) och kortterminal 2 för användare (KT2). En äldre variant av kortterminal för användare, kortterminal 9080 (KT 9080) används ännu. Denna kortterminal kommer att fasas ut i samband med att den nya KT2 fördelas ut till användare.

Observera att kortterminalerna klassificeras som signalskyddsmateriel och därför skall hanteras enligt regler för sådan materiel.

För inläsning av kryptonycklar i det aktiva kortets minnesenhet krävs den särskilda administratörsterminalen, KT ADM.

Bild 14 Kortterminal administration 9090 (KT ADM).

Bild 15 Kortterminal 2 för användare (KT2).

Kapitel 8
Kontroll

Kontroll av signalskyddstjänsten syftar till att säkerställa att regler för signalskyddstjänsten följs samt att signalskyddet är anpassat till det aktuella hotet. Kontroll kan dessutom ses som en del i den fortlöpande signalskyddsutbildningen.

Kontroll av signalskyddstjänsten kan utföras som administrativ kontroll eller som signalkontroll.

8.1 Administrativ kontroll

Administrativ kontroll genomförs som extern eller intern kontroll. Den kan antingen vara planlagd som en grundläggande kontroll eller som en uppföljningskontroll. Vid behov kan särskild kontroll genomföras utan eller med kort förvarning, exempelvis då ett akut problem eller incident uppstått.

8.1.1 Extern kontroll

Vid val av kontrolltyp eftersträvas planlagd kontroll eftersom den i sig blir en signal till att höja nivån på signalskyddstjänsten. Planlagd kontroll förbereds i dialog mellan berörda parter och genomförs vid en överenskommen tidpunkt eller inom en bestämd tidsperiod och omfattar i huvudsak planläggning och säkerhetsskydd för signalskyddstjänsten enligt exempel i bilaga 7.

8.1.2 Internkontroll

Varje myndighet/enhet skall dessutom regelbundet kontrollera den egna signalskyddstjänsten (internkontroll) enligt nedan. Sådan kontroll bör genomföras årligen, förslagsvis i samband med inventering av signalskyddsmaterielen samt vid större personalförändringar som berör signalskyddstjänsten. För mer information se bilaga 8.

> *Varje myndighet skall genomföra kontroll av den egna signalskyddstjänsten. En kontroll skall avse instruktionen och säkerhetsskyddet för signalskyddstjänsten. Det skall finnas en plan för när och hur denna kontroll skall genomföras.*
>
> *Myndigheten skall föra protokoll över varje kontroll. Protokollen skall sparas i minst 10 år.*
>
> *Om myndigheten består av flera enheter gäller vad som föreskrivs i första och andra styckena varje enhet.*
>
> 12 § FFS 2005:2

8.1.3 Genomförande

Den som skall genomföra administrativ kontroll av signalskyddstjänsten eller signalkontroll av signalskyddet skall vara behörig enligt 10 § FFS 2005:2 samt ha genomgått utbildning eller praktik i hur en kontroll skall genomföras.

Kontrollverksamheten grundas på en årligen fastställd plan som omfattar en femårsperiod. Av planen, som rullas årligen, framgår kontrol-

lens omfattning i stort samt tidpunkt eller tidsperiod för kontrollernas genomförande.

Senast en månad före planerad kontroll får den som skall kontrolleras en detaljplan över hur kontrollen kommer att genomföras. Detaljplanen bör omfatta tidpunkt, omfattning och eventuella anvisningar för kontrollens genomförande. Vid behov infordras samtidigt de handlingar som beskriver signalskyddets organisation, kontaktinformation m m vid den myndighet/enhet som skall kontrolleras.

Finns särskild anledning kan kontroll ske utan fastställd plan eller detaljplan.

Kontrollverksamheten bör genomföras i samförstånd, lämpligen i dialogform och på ett sådant sätt att den som kontrolleras uppfattar kontrollen som ett stöd. Varje kontroll bör inledas med en genomgång av kontrollens syfte och omfattning samtidigt som den kontrollerade myndigheten/enheten ges möjlighet att redovisa sin verksamhet och uppgifter.

Det är lämpligt att den som kontrolleras redovisar innehållet i den eller de handling(ar) som beskriver signalskyddets organisation m m (se avsnitt 3.4 ”Dokumentation/planläggning”) innan kontrollen av säkerhetsskyddet för signalskyddstjänsten genomförs.

Direkt efter genomförd kontroll delges en muntlig sammanfattning av gjorda iakttagelser. Vid denna sammanfattning samt vid den inledande genomgången bör chef(er) samt all signalskyddspersonal delta.

Iakttagelser efter genomförd kontroll dokumenteras i ett protokoll. Senast tre månader efter kontrollen, tillsänds den kontrollerade myndigheten/enheten protokollet över gjorda iakttagelser. Av protokollet bör framgå om och när den kontrollerade myndigheten/enheten skall insända rapport över vilka åtgärder som vidtagits och planerats med anledning av vad som påtalats i protokollet samt en tidsplan för åtgärdsarbetet. Av protokollet bör även framgå om och när en uppföljningskontroll kommer att genomföras.

Kontroll av att påtalade fel och brister är åtgärdade bör ske *senast* inom ett år från det att felen och bristerna påtalades.

Ansvar och uppgifter

Varje chef är ansvarig för att signalskyddet inom eget ansvarsområde regelbundet kontrolleras. Allvarliga brister rättas till omedelbart. Övriga brister förtecknas i protokoll, åtgärder planeras för att eliminera bristerna.

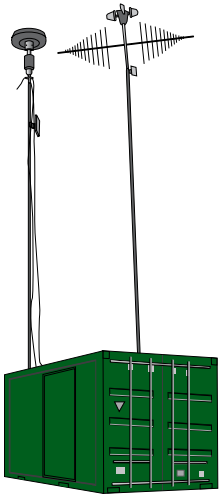
Försvarsmakten

Högkvarteret (TSA), eller den som Högkvarteret utser, genomför administrativa kontroller av signalskyddstjänsten inom Försvarsmakten samt vid civila myndigheter/enheter som tilldelats eller anskaffat signalskyddssystem.

Försvarets materielverk

FMV ansvarar för att signalskyddstjänsten kontrolleras vid försvarsindustrin och vid företag som tagits i anspråk av FMV för utveckling/tillverkning av signalskyddsmateriel samt övriga företag eller motsv som genom lån från FMV erhållit signalskyddsmateriel.

8.2 Signalkontroll



En myndighet skall, om möjligt, se till att signalkontroll genomförs i den omfattning som behövs för att konstatera om signalskyddet är tillräckligt.

Har en myndighet genomfört signalkontroll skall fel eller brister som upptäckts vid kontrollen och som inte är av ringa betydelse anmälas till Högkvarteret.

Varje myndighet som har fått del av resultatet av en signalkontroll skall utan dröjsmål vidta de åtgärder som krävs för att säkerställa signalskyddet.

13 § FFS 2005:2

8.2.1 Grunder

Signalkontroll syftar till att försvåra eller om möjligt förhindra främmande signalunderrättelsetjänst eller annan obehörigs inriktning mot, åtkomst till, störande eller manipulering av information i våra telekommunikations- och IT-system.

Detta genomförs t ex genom att

- klarlägga vilka underrättelser obehöriga kan ha erhållit ur den kontrollerade signaleringen,
- klarlägga obehörigs möjligheter till insyn och intrång i samt påverkan av våra telekommunikations- och IT-system,
- medverka till att stärka signal- och säkerhetsskyddet vid svenska förband utomlands,
- kontrollera att systemen används enligt gällande regler,
- kontrollera att signalskyddssystemen fungerar på avsett sätt,
- i fred medverka till att klarlägga behovet av signalskydd för en bestämd funktion i Sverige och vid internationella insatser av svenska förband,
- vidta åtgärder för att underlätta signalering.

Ovanstående säkerställs genom att den tekniska utvecklingen följs inom områdena telekommunikations- och IT-system samt inom den tekniska utvecklingen avseende nya hot mot avlyssning.

Signalkontroll ingår i IT-säkerhets- och signalskyddstjänst samt säkerhetsunderrättelse- och säkerhetsskyddstjänst.

8.2.2 Genomförande och ansvar

Kontroll av information lagrad på datamedia eller annat lagringsmedia där det framgår att innehållet är av privat karaktär, får endast genomföras om den som förfogar över utrustning/nätverk utfärdat bestämmelser som medger detta. I övriga fall skall meddelande om att sådan kontroll kommer att ske meddelas berörda.

Kontroll av samtal, som utväxlas via telebefordringsföretag inklusive abonnentväxel med tillhörande anknytningar, får endast utföras om minst en av de samtalande känner till att förbindelsen kontrolleras.

Kontroll som utförs på trådförbindelse anslutet till ett telebefordringsföretag skall alltid ske öppet. Övrig kontroll sker öppet om det medges med hänsyn till verksamhetens sekretesskrav. Förbindelse som helt upplåtits eller hyrts för viss verksamhet ingår inte i telebefordringsföretag.

Trafik som förmedlas via Försvarsmaktens IP-nät, exempelvis elektronisk post och FMG, inhämtas av Högkvarteret. Meddelanden som sänds i våra övriga landsomfattande nät/system kontrolleras i samråd med system- och nätansvarig.

Att signalkontroll skall genomföras tillkännages före genomförandet på något eller några av följande sätt.

- Genom arbetsordning, stående order eller liknande dokument.
- På bildskärm eller motsvarande vid inloggning i nätverk.
- I övningsorder.
- Med anslag på telekommunikations- eller IT-system.
- Genom anslag på framträdande plats inom övningslokal eller motsvarande.
- Genom muntlig eller skriftlig information till berörd personal.

Signalkontroll kan begränsas till *signaltjänstkontroll*. Denna form av kontroll används främst för kontroll av signalering som utförs av personal under utbildning.

Resultatet från signalkontroll kan ha stort underrättelsevärde. Åtgärder vidtas för att förhindra att obehörig får tillgång till denna information, såväl under pågående kontroll som vid bearbetning och delgivning.

Högkvarteret (TSA) genomför signalkontroll dels med avseende på verksamhet som kräver högt eller långvarigt skydd mot att sekretessbelagda uppgifter röjs, dels vid ledningsövningar, större övningar, prov- och försöksverksamhet, beredskapskontroller och internationell verksamhet där svenska förband deltar. Signalkontrollen inriktas främst på det verkliga säkerhetsskyddet.

Chef kan genomföra signalkontroll i telekommunikations- och IT-system inom eget ansvarområde.

8.2.3 Inriktning

Signalkontroll inriktas med hänsyn till:

- Betydelsen för främmande signalunderrättelsetjänst eller annan obehörig av den del av trafiken som kan avlyssnas i våra telekommunikations- och IT-system.
- Tekniska möjligheter för obehörig, till insyn och intrång i samt påverkan av våra telekommunikations- och IT-system.
- Möjligheter för obehörig avlyssning av röjande signaler (RÖS).
- Konstaterade brister i sekretesskyddet.
- Obehörigs möjligheter att genom trafikbearbetning få information om sekretessbelagda förhållanden.
- Vidtagna signalskyddsåtgärder.

Vid höjd beredskap kan signalkontrollen dessutom inriktas mot geografiskt område eller särskild verksamhet.

Signalkontroll kan koncentreras under längre tid till visst slag av signalering och viss verksamhet för att samla erforderligt underlag för närmare studier av konstaterade brister. I samband med bearbetning vid sådan signalkontroll bör även trafikbearbetning av textskyddade meddelanden utföras samt anbefalld radiotystnad kontrolleras.

Under övningar bör inledningsskeden och avslutningsskeden särskilt uppmärksammas.

8.2.4 Bearbetning

Omedelbar och långsiktig bearbetning utförs som text-, trafik- och teknisk bearbetning. Den syftar till att klarlägga vilken information med underrättelsevärde som främmande signalunderrättelsetjänst kan ha utvunnit ur våra telekommunikations- och IT-system.

Omedelbar bearbetning syftar till att snabbt klarlägga sådana förhållanden som bör rättas till omgående eller som kan påverka planering av fortsatt verksamhet.

Långsiktig bearbetning sker vid Högkvarteret och syftar till att klarlägga vilka underrättelser obehörig kan ha erhållit genom systematisk uppföljning av vår signalering.

8.2.5 Delgivning

Kontrollerade enheter och kontrollerad personal delges konstaterade brister beträffande signal- och sekretesskydd.

Delgivning kan ske

- i undantagsfall som direkt ingripande i signaleringen vid allvarlig brist i signal- eller sekretesskydd,
- muntligt eller skriftligt omedelbart efter signaleringens slut,
- i form av skrivelse eller rapport efter bearbetning,
- muntligen vid stabsorientering eller annan genomgång,
- i form av sammanställning av kontrolliakttagelser,
- som informationsblad inom egen och underlydande enheter.

Uppgift om att en enstaka viktig underrättelse kan ha kommit till obehörigs kännedom delges omgående ansvarig personal. Delgivning av viktiga iakttagelser får inte fördröjas av formella skäl.

8.2.6 Inrapportering till Högkvarteret

Rapport över resultat från signalkontroll från övningar eller annan verksamhet insänds till Högkvarteret (TSA) om det bedöms ha särskilt intresse eller i övrigt vara av värde för signalskyddstjänsten eller säkerhetstjänsten.

Den som anordnat signalkontroll insänder efter anmodan dessutom

- kontrolljournaler och registrerat innehåll (lagringsmedia),
- rapporter,
- sambands- och säkerhetstjänstorder,
- övningsförutsättningar, samt

- övriga handlingar som bedöms kunna underlätta en allsidig bearbetning av materialet.

Signalkontrolliakttagelser ingår som en del i rapport avseende signalskydds- eller säkerhetsskyddsläget och bör innehålla en sammanställning av viktiga och ofta återkommande iakttagelser.

KAPITEL 9
Signalskydd vid internationell verksamhet

Sveriges utökade internationella åtaganden samt Försvarsmaktens behov av samverkan med andra nationer vid deltagande i internationella insatser, PFP-verksamhet m m, ställer krav på signalskydd även i sådan verksamhet.

Internationell verksamhet ställer höga krav på personalens kompetens och fackkunskaper inom signalskyddstjänsten. Varje tjänsteman blir ofta föremål för någon form av utländsk bedömning. Det är viktigt att svensk personal uppvisar ett gott signalskydds- och säkerhetsmedvetande samt uppträder professionellt i sin roll.

Detta avsnitt tar i huvudsak upp allmänna råd och grundläggande bestämmelser för hantering av signalskyddsmateriel och kryptonycklar vid och inför internationell verksamhet.

Allmänna råd för Försvarsmaktens förband utomlands framgår av särskild skrivelse. Dessa råd kan i tillämpliga delar nyttjas som vägledning för alla myndigheter/enheter som har behov av signalskydd i internationell verksamhet.

9.1 Grundläggande bestämmelser

För att få föra ut och använda kryptonycklar och signalskyddsmateriel i internationell miljö finns följande grundläggande bestämmelser.

> *För att få medföra eller på annat sätt göra kryptonycklar tillgängliga utanför svenskt territorium krävs*
>
> *1. godkännande av Högkvarteret, och*
>
> *2. att den nyckelansvarige i samråd med Högkvarteret har beslutat hur nycklarna skall hanteras.*
>
> 22 § FFS 2005:2

Privata nycklar som ingår i asymmetriska kryptosystem och har signalskyddsgrad SG R (TAK, TEID eller mjuka certifikat) får dock medföras eller på annat sätt göras tillgängliga utanför svenskt territorium utan Högkvarterets godkännande.

> *För att få föra ut signalskyddsmateriel utanför svenskt territorium krävs godkännande av Högkvarteret.*
>
> 28 § FFS 2005:2

9.2 Bestämmelser för utförsel, införsel samt återförsel

9.2.1 Signalskyddsmateriel

För att få använda signalskyddsmateriel utanför svenskt territorium krävs att materielen är godkänd för detta av Högkvarteret (TSA) samt att tillämpningsbestämmelser för hantering är upprättade i samråd med Högkvarteret (TSA).

Utöver ovanstående måste det även finnas tillstånd från Inspektionen för strategiska produkter (ISP) för att få föra ut materielen ur Sverige.

Materiel ingående i signalskyddssystem för personligt bruk *kan under vissa förutsättningar* få medföras utrikes utan särskilt tillstånd. Råd och anvisningar kan erhållas från ISP. Det kan även krävas tillstånd från besökslandet att medföra och nyttja signalskyddsmaterielen samt att få föra materielen ograverad ut ur besökslandet tillbaka till Sverige.

Ingående kryptokomponenter i ett signalskyddssystem är klassificerade som strategiska produkter (dual-use produkter eller krigsmateriel). De är därmed belagda med restriktioner vad avser utförsel enligt lag och förordning om strategiska produkter respektive krigsmateriel.

Varje myndighet/enhet ansvarar själv för att tillstånd söks enligt andra stycket ovan. Inom Försvarsmakten handläggs tillståndsärenden enligt andra stycket ovan av Högkvarterets Protokoll (HKV Prot).

9.2.2 Kryptonycklar

Utöver de ovan angivna grundläggande bestämmelserna enligt 22 § FFS 2005:2 (avsnitt 9.1) beaktas kraven i Säkerhetsskyddsförordningen nedan.

> *”För försändelser med hemliga handlingar till utlandet skall Utrikesdepartementets kurirförbindelser anlitas.*
>
> *Rikspolisstyrelsen och Försvarsmakten kan för sina respektive tillsynsområden enligt 39 § besluta om undantag från första stycket.”*
>
> 11 § säkerhetsskyddsförordningen (1996:633)

Försvarsmaktens förband skall dessutom vad avser internationell verksamhet i tillämpliga delar beakta vad som framgår av Försvarsmaktens föreskrifter om säkerhetsskydd.

9.3 Signalskyddssystem

Det finns i dag två typer av system som är godkända för användning och hantering i internationell verksamhet.

1. I-system som *med vederbörliga avtal* även får användas och hanteras av utländska medborgare.

   Grundkravet är att det på regeringsnivå finns ett utfärdat samarbetsavtal med den aktuella staten samt att säkerhetsskyddsavtal har slutits med den stat som skall vara mottagare av hemlig information (kryptonycklar) och signalskyddsmateriel.

   Vidare krävs ett signalskyddsavtal mellan Försvarsmakten (TSA/NCSA) och den aktuella statens motsvarande funktion som i *varje* särskilt fall reglerar

   - signalskyddets ledning och organisation,
   - krav på utbildning och behörighet,
   - hantering av kryptonycklar vad avser mottagning, distribution, delgivning, förvaring och förstöring,
   - åtgärder vid signalskyddsincident,
   - hantering av signalskyddsmateriel vad avser placering, förvaring och förlust,
   - när och hur signalskyddsmaterielen skall återlämnas.

   När ett avtal enligt ovan skall skrivas och förhandlas skall avtalet godkännas av Högkvarteret (TSA).
2. U-system som endast får användas och hanteras av personal anställd vid svensk statlig myndighet eller vid svenskt företag som har tecknat avtal om signalskydd.

Högkvarteret (TSA/NCSA) skall vara delaktiga i avtalsprocessens samtliga delar, från förhandling till undertecknande.

Upplysning om vilka system, av de två typerna, som finns tillgängliga för användning kan erhållas från Högkvarteret (TSA/NCSA). Avtalen skall vara godkända och undertecknade av båda parter innan utbildning av utländsk personal kan påbörjas, eller transport av signalskyddsmateriel och kryptonycklar till annat land genomförs.

9.3.1 Annan stats signalskyddssystem

För svensk myndighet/enhet som tilldelats annan stats signalskyddssystem, gäller de bestämmelser – avseende hantering av materiel och kryptonycklar – som framgår av det särskilda avtal som upprättats mellan de berörda länderna.

Signalskyddssystem för samverkan, som tilldelats myndigheten/enheten som lån från annan stat, får endast användas för information i enlighet med de sekretessbestämmelser som framgår av avtalet. När ett sådant avtal skall skrivas och förhandlas skall avtalet godkännas av Högkvarteret (TSA).

Bilaga 1

Signalskyddsbedömande

Ett signalskyddsbedömande (inom Försvarsmakten) bör ligga till grund för utarbetandet av planer/instruktioner och order för signalskyddstjänsten.

Signalskyddsbedömandet syftar till att klarlägga det aktuella hotet och våra möjligheter att genom olika signalskyddsåtgärder minska verkan av motståndarens informationsoperationer.

Exempel på disposition av ett signalskyddsbedömande:

1. *Redovisa högre chefs beslut i stort och inriktning samt enhetens uppgift,* detta för att klarlägga signalskyddstjänstens mål och uppgifter.
2. *Överväg informationsoperationernas påverkan på våra ledningssystem*, utifrån motståndarens
   - organisation och gruppering,
   - möjligheter till avlyssning, lokalisering, identifiering samt övrig trafikanalys,
   - tidsförhållanden för bearbetning och delgivning samt
   - störsändning och falska signalering.
3. *Redovisa aktuellt signalskyddsläge,* resurser och handlingsmöjligheter med fördelar och nackdelar utifrån
   - materiel- och personalläge,
   - kryptonyckelläge, avseende tilldelning, distribution och nyckelincidenter,
   - möjligheterna till radiotystnad, identifierings- och lokaliseringsförsvårande åtgärder, behörighetskontroll, skydd mot störsändning samt
   - disponibla signalkontrollresurser.

Bilaga 2

Riktlinjer vid sekretessbedömning av uppgifter inom totalförsvarets signalskyddsverksamhet

Den som upprättar en handling har ansvaret för att en korrekt sekretessbedömning av uppgifterna görs. Då det kan vara svårt att bedöma om en uppgift omfattas av sekretess enligt sekretesslagen (1980:100), har denna bilaga med riktlinjer för sekretessbedömning tagits fram. Riktlinjerna syftar till att tjäna som stöd vid bedömning rörande uppgifter om totalförsvarets signalskyddsverksamhet.

Med stöd av dessa riktlinjer kan värdering av om en uppgift omfattas av sekretess göras. Riktlinjerna i denna bilaga tar ingen hänsyn till om uppgiften rör rikets säkerhet eller inte. För att förtydliga detta anges i riktlinjerna ”hemligt eller sekretessbelagt” för att visa på att uppgiften kan röra rikets säkerhet men inte behöver göra det. Det är den som upprättar en handling där uppgiften förekommer som skall bedöma om uppgiften rör rikets säkerhet eller inte.

Sekretessbedömning utförs i regel mot 2 kap 2 § sekretesslagen, den s k försvarssekretessen. Sekretessbedömning kan även göras mot andra lagrum t ex 2 kap 1 §, den s k utrikessekretessen, och 5 kap 2 och 3 §§ sekretesslagen, som rör säkerhets- bevakningsåtgärder samt chiffer m m.

Ytterligare vägledning vid sekretessbedömning kan fås ur ”Handbok för Försvarsmaktens Säkerhetsskyddstjänst Sekretessbedömning” H SÄK Sekrbed.

Signalskyddsmetoder

Kryptering och dekryptering

Offentligt kan vara:

- Principiella metoder för kryptering.

Hemligt eller sekretessbelagt är normalt:

- Upptäckta fel och brister.
- Ifylld kodordstabell.

Täckning

Offentligt kan vara:
- Metoder för täckning.

Hemligt eller sekretessbelagt är normalt:
- Täcktabell försedd med nyckel.
- Blankett som innehåller både klartext och täckterm.
- I vissa fall ordmassa.

Omskrivning

Offentligt kan vara:
- Metoder för omskrivning.

Hemligt eller sekretessbelagt är normalt:
- Hänvisningshandling (den handling som man har hämtat termer för omskrivning ur).

Trafikskydd

Offentligt kan vara:
- Metoder för trafikskydd.

Hemligt eller sekretessbelagt är normalt:
- Order och omfattning av radiotystnad.
- Planläggning av sändares placering.
- Meddelande om planering, genomförande, rapportering och övriga omständigheter som berör en provsändning.
- Rörliga anropssignaler.
- Tillfälliga anropssignaler.
- Uppgifter rörande planerad, pågående eller utförd fyllnadssignalering.
- Planlagda skyddsåtgärder mot störsändning.
- Plan för frekvensbyte.

Val av signalskydd

Offentligt kan vara:

- Metoder.

Hemligt eller sekretessbelagt är normalt:

- Kryptosambandstablåer med nyckelseriebeteckning utskriven i klartext.

Ledning och samordning

Planläggning

Offentligt kan vara:

- Förekomsten av planläggning.
- Enskild myndighets/enhets signalskyddsutbildade personal och dess behörighet.
- Enskild myndighets/enhets sammanställning av tilldelad signalskyddsmateriel.

Hemligt eller sekretessbelagt är normalt:

- Signalskyddsbedömande.
- Särskilda åtgärder som skall vidtas vid höjd beredskap.
- Sammanställning av tilldelade nyckelserier (kryptonycklar) samt var och hur dessa förvaras.
- Enskild myndighets/enhets placering eller förvaring av signalskyddsmateriel.

Utbildning

Dokumentation av genomförd utbildning

Offentligt kan vara:

- Förekomsten av register över utbildad personal.

Hemligt eller sekretessbelagt är normalt:

- Sammanställningar över flera myndigheters/enheters signalskyddsutbildade personal.

Signalskyddssystem

Godkännande

Offentligt kan vara:
- Rutiner för godkännande.

Hemligt eller sekretessbelagt är normalt:
- Kryptoverifieringsplan.
- Säkerhetsgranskning.
- Resultat från RÖS-mätning.
- Algoritm i form av källkod.

Kvalificerat hemligt eller sekretessbelagt är normalt:
- Påvisade svagheter i den kryptologiska styrkan hos ett signalskyddssystem.

Kryptonycklar

Offentligt kan vara:
- Testnycklar.
- Systembeteckning.
- Kryptobeteckning (Krybet).

Hemligt eller sekretessbelagt är normalt:
- Kryptonycklar.
- Nyckelns seriebeteckning.
- Kryptobeteckningsregister.
- Tilldelning av nyckelserie.
- En myndighets/enhets samlade behov av nycklar.
- Beställning av nycklar.
- Programvara för nyckelproduktion.
- Produktionsmetoder.
- Kvitton/följesedlar.
- Driftsättning av nyckelserie/nycklar.

- Anmälan om nyckelincident.
- Meddelande om åtgärder vid nyckelincidenter.
- Förstöringsliggare för nycklar.

Nyckelinjektor

Offentligt kan vara:
- Metoder för användning.

Hemligt eller sekretessbelagt är normalt:
- Nyckelinjektor med inlästa nycklar.
- PIN till nyckelinjektor intill dess att den används.
- Blankett med engångs-PIN.

Nyckelserver

Offentligt kan vara:
- Metoder för användning.

Hemligt eller sekretessbelagt är normalt:
- Nyckelserver med inläst hemlig information.

Signalskyddsmateriel

Offentligt kan vara:
- Materiel utan inläst kryptonyckel.
- Avveckling av materiel.

Hemligt eller sekretessbelagt är normalt:
- Materiel med inläst kryptonyckel.
- Materiel med bruten plombering.
- Plomberingsprotokoll.
- Anmälan om förlust av signalskyddsmateriel.
- Sammanställning över fördelad materiel.

Aktiva kort/mjuka certifikat (TAK, NBK, TEID)

Offentligt kan vara:

- Metoder och användning av aktiva kort eller mjuka certifikat.
- Aktivt kort, dock skall det hanteras så att innehavaren ständigt har kontroll över kortet.
- Beställning av aktiva kort och certifikat, dock skall beställningen ske på ett säkert sätt.
- Certifikat.
- Anmälan om förlust av aktivt kort, dock skall anmälan ske på ett säkert sätt.
- Kvitto för aktivt kort.

Hemligt eller sekretessbelagt är normalt:

- Privat RSA-nyckel.
- PIN/PUK.
- Aktivt kort med inläst kryptonyckel.

Kontroll

Administrativ kontroll

Offetnligt kan vara:

- Att kontroller genomförs.

Hemligt eller sekretessbelagt är normalt:

- Protokoll efter genomförd kontroll.

Signalkontroll

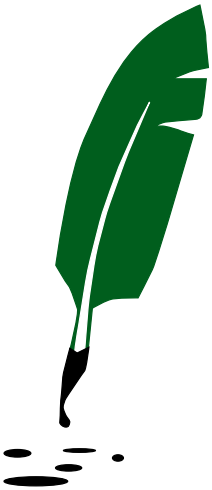
Offentligt kan vara:

- Att signalkontroll genomförs under övning
- Att signalkontroll genomförs regelmässigt i FM landsomfattande nät.

Hemligt eller sekretessbelagt är normalt:

- Att signalkontroll genomförs under verksamhet som kräver sekretess.
- Rapport över resultat av signalkontroll.
- Registrerat innehåll i avlyssnad trafik.
- Signalkontrollens totala resurser att genomföra kontroll.

Bilaga 3



Exempel på disposition av en fullständig signalskyddsinstruktion

Allmänt

- Upprättande och fastställande av signalskyddsinstruktion.
- Delgivning.
- Syfte.
- Beredskapskrav.
- Revideringsintervall.

Hotbild

- Orientering om olika hot mot våra telekommunikations- och IT-system, t ex signalspaning, störsändning och falsk signalering.

Förteckning över styrande dokument och publikationer

- Försvarsmaktens föreskrifter (FFS) om signalskyddstjänsten inom totalförsvaret.

- H TST Grunder.
- Systeminstruktioner för respektive signalskyddssystem.
- Annan signalskyddsspecifik information.
- Myndighetens/enhetens egna föreskrifter, arbetsordning etc där signalskydd omnämns.

Signalskyddsorganisation och personal

- Signalskyddets organisation vid grundberedskap, fredstida krishantering och höjd beredskap.
- Aktuell personal.
- Hur signalskyddet upprätthålls vid ordinarie befattningshavares frånvaro.

Utbildning

- Detaljerad utbildningsförteckning över samtlig signalskyddsutbildad personal omfattande givna behörigheter, omfattning av och tidpunkt för utbildningen samt kursanordnande skola/lärare/behörig utbildare.

Materiel

- Förteckning över signalskyddsmateriel med angivande av individnummer samt uppgift om var signalskyddsmaterielen förvaras (rumsnummer eller motsv och ev säkerhetsskåp). Förteckningen skall ständigt hållas aktuell.
- Åtgärder vid förlust eller åverkan på utrustning eller plombering.
- Rutiner vid ersättning, underhåll och reparation av signalskyddsmateriel.
- Uppgift om hur förbrukningsmateriel erhålls.
- Information om till annan myndighet/enhet utlånad signalskyddsmateriel, inklusive överenskommelse eller avtal om hur materielen skall återföras.

Kryptonycklar

- Uppgift om hur myndigheten/enheten försörjs med kryptonycklar.
- Uppgift om vilka åtgärder som skall vidtas då kryptonycklar inte kommit myndigheten/enheten tillhanda inom föreskriven tid.
- Förteckning över tilldelade kryptonyckelserier.
- Flödesschema eller punktlista omfattande kryptonyckels
  - beställning,
  - mottagning/registrering,
  - distribution,
  - delgivning/inläsning,
  - förvaring,
  - rutinmässig förstöring (inkluderande information om godkänd pappersdestruktör och dess placering).
- Regler/rutin för förande av trafiklista.

Aktiva kort/mjuka certifikat

Flödesschema eller punktlista omfattande aktiva korts/mjuka certifikats

- beställning,
- mottagning/registrering,
- förteckning över tilldelade aktiva kort/mjuka certifikat,
- distribution,
- delgivning,
- hantering,
- förvaring,
- återsändning/revokering/förstöring.

Kryptosambandstablå

- Sammanställning av enhetens möjlighet att med hjälp av signalskyddssystem och nyckelserier överföra krypterad information med samverkande myndigheter/enheter.

Åtgärder vid misstanke om signalskyddsincident

- Uppgifter om åtgärder vid misstanke om nyckelincident eller materielincident vid egen myndighet/enhet.
- Uppgifter om åtgärder vid meddelande om nyckelincident eller materielincident vid annan myndighet/enhet.
- Uppgifter om åtgärder vid förlust av eller obehörig åtkomst till aktiva kort/mjuka certifikat.

Begränsad respektive total förstöring

- Uppgifter om
  - åtgärder vid begränsad förstöring,
  - åtgärder vid total förstöring,
  - vem som beordrar och genomför förstöringen,
  - hur förstöringen genomförs.

Åtgärdskalender

- Uppgift om vilka åtgärder som skall vidtas vid olika beredskapshöjningar.
- Hur och med vilken regelbundenhet skall myndigheten/enheten genomföra internkontroller?

Kontaktpersoner vid egen eller andra myndigheter/enheter

Bilaga 4. Krav för signalskyddssystem avsedda för Totalförsvaret

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum	HKV beteckning
2007-03-27	12 830: 65517

Sändlista

Ert tjänsteställe, handläggare	Ert datum	Er beteckning

Vårt tjänsteställe, handläggare	Vårt föregående datum	Vår föregående beteckning
Pia Gruvö, MUST SÄKK TEK Kry, 08 - 788 7799 pia.gruvo@mil.se	2004-03-05	12 830: 63928

Krav för signalskyddssystem avsedda för Totalförsvaret
(En bilaga)

Enligt Säkerhetsskyddsförordningen (1996:633), 13 § gäller följande: *Hemliga uppgifter får krypteras endast med kryptosystem som har godkänts av Försvarsmakten.*

I 4 § förordningen (2000:555) med instruktion för Försvarsmakten framgår att Försvarsmakten skall leda och samordna signalskyddstjänsten inklusive arbetet med säkra kryptografiska funktioner inom totalförsvaret. I 39 § samma förordning framgår att FM får meddela övriga statliga myndigheter föreskrifter i frågor om signalskyddstjänsten inklusive säkra kryptografiska funktioner inom totalförsvaret.

Verkställande organ för FM ledning och samordning är totalförsvarets signalskyddssamordning (TSA) som är en funktion inom säkerhetskontoret (SÄKK) vid militära underrättelse- och säkerhetstjänsten (MUST) i Högkvarteret (HKV).

I bilaga specifieras övergripande de krav som ligger till grund för att ett signalskyddssystem skall kunna bli godkänt. Kraven avser sekretesskydd för olika signalskyddsgrader, autentisering samt integritetsskydd. ./ .

Följande bilaga fastställes för att ligga till grund vid upphandling och utveckling av system som nyttjar kryptografiska metoder som skyddsmekanism vid hantering av hemliga uppgifter och ersätter tidigare skrivelse i detta ärende.

(pgö)

Postadress	Besöksadress	Telefon	Telefax	E-post, Internet
107 85 STOCKHOLM	Lidingövägen 24	08-788 75 00	08-788 77 78	exp@hkv.mil.se www.hkv.mil.se

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

HKV beteckning
12 830: 65517

Beslut i detta ärende har fattats av John Daniels, Chef för Säkerhetskontoret. I den slutliga handläggningen har dessutom deltagit Ulf Helgeson och Jan-Ove Larsson och som föredragande varit Pia Gruvö.

John Daniels

Pia Gruvö

Sändlista

FMV	(3 ex, varav ett ex avsett för MSL 466 och ett ex avsett för FMV: Signalskydd)
FRA	
KBM	
FOI	
RPS/SÄPO	

Som orientering

S1	(avsett för TSS)

Inom HKV

SP CIO-processen	
FÖRBE ARMÉ	
FÖRBE MARIN	
FÖRBE FV	
FÖRBE LED	
FÖRBE LED Infohantering	(avsett för Arne Olsson)
MUST SÄKK SÄKA	
MUST SÄKK SÄKS	
MUST SÄKK TEK	

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830:65517

Krav för signalskyddssystem ver 1.1

(pgö)

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

1. Inledning

Detta dokument syftar till att beskriva de krav som ställs på signalskyddssystem vad avser sekretess, integritet och autentisering. Kraven redogörs översiktligt och syftar till att ge en inriktning och skall inte betraktas som en komplett kravlista. Krav kan tillkomma eller ändras beroende på vilka typer av system och verksamhetskrav som avses.

2. Lagrum

Enligt Säkerhetsskyddsförordningen (1996:633), 13 § gäller följande: *Hemliga uppgifter får krypteras endast med kryptosystem som har godkänts av Försvarsmakten.*

I 4 § förordningen (2000:555) med instruktion för Försvarsmakten framgår att Försvarsmakten skall leda och samordna signalskyddstjänsten inklusive arbetet med säkra kryptografiska funktioner inom totalförsvaret. I 39 § samma förordning framgår att FM får meddela övriga statliga myndigheter föreskrifter i frågor om signalskyddstjänsten inklusive säkra kryptografiska funktioner inom totalförsvaret.

Verkställande organ för FM ledning och samordning är totalförsvarets signalskydds-samordning (TSA) som är en funktion inom säkerhetskontoret (SÄKK) vid militära underrättelse- och säkerhetstjänsten (MUST) i Högkvarteret (HKV).

Enligt FFS 2005:2, 4 § gäller följande: *Ett signalskyddssystem som är avsett för skydd av uppgifter som omfattas av sekretess enligt sekretesslagen (1980:100) skall i samband med Högkvarterets godkännande placeras i någon av nedan angivna signalskyddsgrader med följande beteckningar och betydelser.*

Signalskyddsgrad	**Betydelse**
SG TS	Signalskyddssystemet är godkänt för att behandla information som 1. är kvalificerat hemlig, 2. hänförs till informationssäkerhetsklassen HEMLIG/TOP SECRET, 3. internationellt är klassad TOP SECRET, eller 4. om den röjs skulle förorsaka totalförsvaret eller förhållandet till annat land eller mellanfolklig organisation synnerligt men.
SG S	Signalskyddssystemet är godkänt för att behandla information som 1. är hemlig, men inte kvalificerat hemlig, 2. hänförs till informationssäkerhetsklassen HEMLIG/SECRET, 3. internationellt är klassad SECRET, eller 4. om den röjs skulle förorsaka totalförsvaret eller förhållandet till annat land eller mellanfolklig organisation betydande, men inte synnerligt, men.
SG C	Signalskyddssystemet är godkänt för att behandla information som 1. hänförs till informationssäkerhetsklassen HEMLIG/CONFIDEN-TIAL, 2. internationellt är klassad CONFIDENTIAL, eller

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

3. om den röjs skulle förorsaka totalförsvaret eller förhållandet till annat land eller mellanfolklig organisation inte obetydligt, men inte betydande eller synnerligt, men.

SG R

Signalskyddssystemet är godkänt för att behandla information som
1. hänförs till informationssäkerhetsklassen HEMLIG/RESTRICTED,
2. internationellt är klassad RESTRICTED, eller
3. om den röjs skulle förorsaka totalförsvaret eller förhållandet till annat land eller mellanfolklig organisation endast ringa men.

Enligt Försvarsmaktens interna bestämmelser gäller dessutom att innan ett signalskyddssystem tas i drift skall det ha godkänts av chefen för militära underrättelse- och säkerhetstjänsten i Högkvarteret eller den han har bestämt. Ett godkännande skall dokumenteras.

Vidare gäller enligt samma bestämmelser att den som i Högkvarteret ger eller har uppdrag att utveckla ett signalskyddssystem eller ett informations- eller telekommunikationssystem i vilket kryptografisk funktion avses ingå skall, innan utvecklingen påbörjas, samråda med militära underrättelse- och säkerhetstjänsten i Högkvarteret.

Signalskyddssystem definieras i FFS 2005:2, 3 § som
- system med kryptografiska funktioner som är godkänt av Högkvarteret, och
- system för skydd mot signalunderrättelsetjänst, störsändning eller falsk signalering som är godkända av Högkvarteret.

Kryptografiska funktioner definieras i samma paragraf som metoder och principer för
- skydd av information mot insyn vid överföring och lagring med hjälp av kryptering,
- identifiering och autentisering, och
- signering och verifiering av information.

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

3. Krav för sekretess

SG R (Restricted)

Följande krav måste vara uppfyllda för att ett signalskyddssystem skall kunna godkännas för SG R (Restricted):

Funktionskrav – SGR3-1

Krav-id	Kravbeskrivning	Anmärkning
SGR3-1-1	Kryptering skall ske med en symmetrisk algoritm. Denna skall vara för ändamålet godkänd av TSA samt nyttjas på ett av TSA godkänt sätt. Algoritmen kan vara hemlig *alternativt* vara en allmänt erkänd publik algoritm som motstått omfattande kryptoanalys, till exempel AES (Advanced Encryption Standard).	
SGR3-1-2	Systemet skall använda nyckelgenererings- och slumptalsalgoritmer som skall godkännas av TSA.	
SGR3-1-3	Kryptonycklar skall kunna raderas och bytas med enkla rutiner.	
SGR3-1-4	Nycklar på separat lagringsmedia skall eftersträvas.	
SGR3-1-5	Det kryptologiska systemet skall vara godkänt av TSA (exempelvis algoritm, nyckelhantering och kryptologiska protokoll).	
SGR3-1-6	Det kryptologiska systemet skall skyddas mot obehörig åtkomst och manipulation minst lika väl som den information kryptot avser att skydda.	
SGR3-1-7	För system som är anslutet till radioutrustning eller placerat i radioutrustningens omedelbara närhet skall risk för RÖS beaktas.	
SGR3-1-8	Systemet kan använda asymmetriska metoder för nyckelutbyte och dessa skall för ändamålet vara godkända av TSA. Generellt gäller att publika nycklar skall hanteras med Försvarsmaktens PKI, där certifikat och nycklar beställs från TSA.	

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

Assuranskrav SGR3-2

Krav-id	Kravbeskrivning	Anmärkning
SGR3-2-1	Följande dokumentation skall levereras till TSA: • Security Target eller motsvarande • Högnivåbeskrivning av det kryptologiska systemet. • Lågnivåbeskrivning av samtliga kryptografiska mekanismer och protokoll. • Källkod för alla komponenter med kryptografiska mekanismer • Kryptoverifieringsplan som skall godkännas av TSA.	
SGR3-2-2	TSA skall tilldelas en referens av systemets kryptorelaterade delar.	
SGR3-2-3	Kryptoverifiering skall utföras och godkännas av TSA. Detta innebär att ett komplett system måste göras tillgängligt för praktiska tester.	
SGR3-2-4	Systemet skall vara säkerhetsgranskat av en oberoende instans. I granskningsrapporten skall ingå säkerhetsmålsättning, penetrationstester samt källkodsgranskning av säkerhetskritiska komponenter. Fullständig granskningsrapport från säkerhets-granskningen skall levereras till TSA.	

SG C (Confidential)

Följande krav måste vara uppfyllda för att ett signalskyddssystem skall kunna godkännas för SG C (Confidential):

Funktionskrav SGC3-3

Krav-id	Kravbeskrivning	Anmärkning
SGC3-3-1	Kryptering skall ske med en symmetrisk algoritm. Denna skall vara för ändamålet godkänd av TSA samt nyttjas på ett av TSA godkänt sätt. Hemlig algoritm skall eftersträvas.	
SGC3-3-2	Endast kryptonycklar tillverkade av TSA eller på ett av TSA godkänt sätt skall användas.	
SGC3-3-3	Kryptonycklar skall kunna raderas och bytas med enkla rutiner. Det skall finnas möjlighet till nödradering.	
SGC3-3-4	Det kryptologiska systemet skall vara godkänt av TSA (exempelvis algoritm, nyckelhantering och kryptologiska protokoll).	
SGC3-3-5	Implementering av algoritmen i hårdvarukrets med separat fysiskt gränssnitt för nyckelinläsning skall eftersträvas.	
SGC3-3-6	Röd/svart-separering skall eftersträvas.	
SGC3-3-7	Det kryptologiska systemet skall konstrueras så att utläsning av nycklar och algoritm samt manipulation av systemet är omöjligt utan att bryta upp kryptoapparat eller motsvarande.	
SGC3-3-8	Kryptoapparat eller motsvarande skall vara RÖS-godkänd enligt nivå U1.	
SGC3-3-9	Kryptoapparat eller motsvarande skall vara förseglad eller plomberad så att personal som hanterar materielen kan konstatera om den utsatts för manipulering.	

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

Assuranskrav SGC3-4

Krav-id	Kravbeskrivning	Anmärkning
SGC3-4-1	Följande dokumentation skall levereras till TSA: ▪ Security Target ▪ Högnivåbeskrivning av det kryptologiska systemet. ▪ Lågnivåbeskrivning av samtliga kryptografiska komponenter, mekanismer och protokoll. ▪ Kryptoverifieringsplan som skall godkännas av TSA. ▪ Källkod för alla ingående komponenter. Undantag kan ges för icke säkerhetskritiska COTS-komponenter.	
SGC3-4-2	TSA skall tilldelas en referens av systemets kryptorelaterade delar.	
SGC3-4-3	Kryptoverifiering skall utföras och godkännas av TSA. Detta innebär att ett komplett system måste göras tillgängligt för praktiska tester	
SGC3-4-4	Systemet skall av en oberoende instans vara säkerhetsgranskat motsvarande CC EAL4+. Utökningen skall bestå av penetrationstester och källkodsgranskning. Fullständig granskningsrapport samt tillhörande underlag skall levereras till TSA.	

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

SG TS (Top Secret) och SG S (Secret)

Följande krav måste vara uppfyllda för att ett signalskyddssystem skall kunna godkännas för SG TS (Top Secret) och SG S (Secret):

Funktionskrav SGS3-5

Krav-id	Kravbeskrivning	Anmärkning
SGS3-5-1	Kryptering skall ske med symmetrisk algoritm. Denna skall vara godkänd av TSA samt nyttjas på ett av TSA godkänt sätt. Algoritmen skall vara hemlig om inte särskilda skäl föreligger.	
SGS3-5-2	Endast kryptonycklar tillverkade av TSA eller på ett av TSA godkänt sätt skall användas.	
SGS3-5-3	Kryptonycklar skall kunna raderas och bytas med enkla rutiner. Det skall finnas möjlighet till nödradering.	
SGS3-5-4	Det kryptologiska systemet skall vara godkänt av TSA (exempelvis algoritm, nyckelhantering och kryptologiska protokoll).	
SGS3-5-5	Inläsning av nycklar i klartext skall ske genom separata fysiska gränssnitt.	
SGS3-5-6	Kryptoapparat eller motsvarande skall designas utifrån principerna för röd/svart-separering.	
SGS3-5-7	Det kryptologiska systemet skall implementeras så att utläsning av nycklar och algoritm i praktiken är omöjligt (Tamper Protection), samt så att manipulation av systemet utan upptäckt är omöjligt (Tamper Evident). Kryptoapparat eller motsvarande skall vara konstruerad så att den som hanterar materielen kan konstatera om apparaten utsatts för manipulering.	
SGS3-5-8	Kryptoapparat eller motsvarande skall vara RÖS-godkänd enligt nivå U1.	
SGS3-5-9	Det kryptologiska systemet skall implementeras i hårdvara. Med hårdvara avses icke omprogrammeringsbara kretsar. I undantagsfall kan omprogrammeringsbara kretsar tillåtas förutsatt att dess	

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

	program/konfiguration enbart kan laddas av TSA.	

Mer detaljerade krav finns beskrivna i skrivelse HKV 12 837: 71695, ”Krav på krypto vid utveckling och upphandling”, 2000-08-31.

Assuranskrav SGS3-6

Krav-id	Kravbeskrivning	Anmärkning
SGS4-6-1	Följande dokumentation skall levereras till TSA: • Security Target • Högnivåbeskrivning av det totala systemet. • Lågnivåbeskrivning av samtliga i systemet ingående komponenter • Kryptoverifieringsplan som skall godkännas av TSA. • Källkod för alla ingående komponenter.	
SGS4-6-2	TSA skall tilldelas en referens av det totala systemet.	
SGS4-6-3	Kryptoverifiering skall utföras och godkännas av TSA. Detta innebär att ett komplett system måste göras tillgängligt för praktiska tester.	
SGS4-6-4	Systemet skall av en av TSA godkänd oberoende instans vara säkerhetsgranskat motsvarande CC EAL4+. Utökningen skall bestå av penetrationstester och källkodsgranskning. Fullständig granskningsrapport samt tillhörande underlag skall levereras till TSA.	

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

Intrångsskydd

Kryptoapparat eller motsvarande kan användas som intrångsskydd till slutna system under förutsättning att den

- ansluts på linjen
- har minst två separata fysiska gränssnitt (det vill säga klartext- och kryptogränssnitt)
- saknar möjlighet till klartextkommunikation mellan de två gränssnitten
- är utformad för att spegla en hotbild för intrång.

För övrigt gäller kraven för signalskyddsgrader. Till exempel, ett signalskyddssystem som är godkänt för signalskyddsgrad *confidential* skulle kunna utgöra ett intrångsskydd för ett nät eller ett system med uppgifter som skulle medföra högst icke obetydligt men vid avslöjande (för Försvarsmakten för uppgifter placerade i informationssäkerhetsklass HEMLIG/CONFIDENTIAL).

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

4. Krav för inloggning och autentisering

För inloggning och autentisering finns två kravnivåer: förstärkt inloggning och stark autentisering. Vilken kravnivå som gäller beror på vilket typ av information som hanteras i systemet, vilka krav på spårbarhet som ställs samt hur homogen användargruppen är med avseende på behörigheter till systemets resurser och information.

Kraven i detta kapitel gäller för inloggning och autentisering i system i syfte att få tillgång till information och resurser. Det beaktar inte kraven för oavvislighet.

Förstärkt inloggning

Följande krav måste vara uppfyllda för att ett system för inloggning och autentisering skall kunna godkännas för Förstärkt inloggning:

Funktionskrav FI4-1

Krav-id	Kravbeskrivning	Anmärkning
FI4-1-1	Användare skall förses med en personlig och unik identitet samt tillhörande inloggningsdata (koder, lösenord, nycklar eller motsvarande). Nyttjande av TEID (Totalförsvarets Elektroniska ID-kort) skall eftersträvas.	
FI4-1-2	Systemet skall ha möjlighet att reagera på upprepade felaktiga inloggningsförsök.	
FI4-1-3	Systemet skall enkelt kunna revokera inloggningsdata om dessa bedöms vara röjda.	
FI4-1-4	Inloggningsdata får inte skickas i klartext.	
FI4-1-5	Enbart lösenord får inte användas.	
FI4-1-6	Algoritmer och slumptalsgenerering i samband med inloggning skall kunna accepteras av TSA.	
FI4-1-7	Inloggningsdata skall ges ett tillfredsställande skydd mot obehörig avläsning och modifiering.	
FI4-1-8	Systemet skall ge ett tillfredställande skydd mot att en inloggad session eller motsvarande kan nyttjas av någon obehörig.	

Assuranskrav FI4-2

Krav-id	Kravbeskrivning	Anmärkning
FI4-2-1	Följande dokumentation skall levereras till TSA: • Högnivåbeskrivning av det kryptologiska systemet. • Lågnivåbeskrivning av samtliga kryptografiska mekanismer och protokoll.	
FI4-2-2	Kryptokontroll skall utföras av TSA. Detta innebär att ett komplett system måste göras tillgängligt för praktiska tester.	
FI4-2-3	Systemet skall vara säkerhetsgranskat av en oberoende instans. Granskningsrapporten skall omfatta säkerhetsmålsättning, penetrationstester samt källkodsgranskning av säkerhetskritiska komponenter. Fullständig rapport från säkerhetsgranskningen skall delges TSA.	

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

Stark autentisering

Följande krav måste vara uppfyllda för att ett system för inloggning och autentisering skall kunna godkännas för Stark autentisering:

Funktionskrav SA4-3

Krav-id	Kravbeskrivning	Anmärkning
SA4-3-1	Användare skall förses med en personlig och unik identitet samt tillhörande inloggningsdata (koder, lösenord, nycklar eller motsvarande).	
SA4-3-2	Systemet skall ha möjlighet att reagera på upprepade felaktiga inloggningsförsök.	
SA4-3-3	Systemet skall enkelt kunna revokera inloggningsdata om dessa bedöms vara röjda.	
SA4-3-4	Algoritmer och slumptalsgenerering i samband med inloggning skall vara godkända av TSA.	
SA4-3-5	Kryptografiska algoritmer och protokoll godkända av TSA skall användas.	
SA4-3-6	Koder, kryptografiska nycklar och algoritmer skall förvaras på godkänt separat medium (lämpligen TAK – Totalförsvarets Aktiva Kort).	
SA4-3-7	Nycklar och certifikat skall beställas från TSA.	
SA4-3-8	Om certifikat används skall dessa alltid verifieras mot aktuell revokeringslista.	
SA4-3-9	Kryptoapparat, kortläsare eller motsvarande skall vara RÖS-godkänd enligt nivå U1. Särskild vikt läggs vid PIN- och nyckelhantering.	
SA4-3-10	All information som utväxlas i starkt autentiserad session eller motsvarande skall knytas till rätt avsändare med hjälp av en godkänd kryptografisk mekanism.	
SA4-3-11	Nyttjande av befintliga TSA-godkända komponenter skall eftersträvas.	

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

Assuranskrav SA4-4

Krav-id	Kravbeskrivning	Anmärkning
SA4-4-1	Följande dokumentation skall levereras till TSA: • Högnivåbeskrivning av det kryptologiska systemet. • Lågnivåbeskrivning av samtliga kryptografiska komponenter, mekanismer och protokoll. • Kryptoverifieringsplan som skall godkännas av TSA. • Källkod för alla ingående komponenter. Undantag kan ges för icke säkerhetskritiska COTS-komponenter.	
SA4-4-2	TSA skall tilldelas en referens av systemets krypto-relaterade delar.	
SA4-4-3	Kryptoverifiering skall utföras av TSA. Detta innebär att ett komplett system måste göras tillgängligt för praktiska tester.	
SA4-4-4	Systemet skall vara säkerhetsgranskat, av en av TSA godkänd oberoende instans, motsvarande CC EAL4+, där utökningen består av penetrationstester och källkodsgranskning. Fullständig granskningsrapport samt tillhörande underlag från säkerhetsgranskningen skall levereras till TSA.	

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

5. Krav för integritet

Med integritetsskydd menas kryptografiska mekanismer för att upptäcka avsiktlig eller oavsiktlig modifiering av information. Hur upptäckten skall hanteras måste definieras för varje system. Exempel på hantering kan vara att ignorera informationen, att logga händelsen eller att larma. Det bör också finnas mekanismer för att återskapa orginaldata vid små fel. För integritetsskydd finns två kravnivåer: medium och hög.

Kraven på integritet styrs från systemets övergripande krav på korrekt och tillförlitlig information. Dessutom kan integritetskraven kopplas mot systemets krav på tillgänglighet, där ett otillräckligt skydd mot avsiktlig eller oavsiktlig modifiering även kan få konsekvenser för systemets tillgänglighet.

Notera att detta dokument inte beaktar krav för oavvislighet.

Kravnivå medel

Följande krav måste vara uppfyllda för att ett system för integritetsskydd skall kunna godkännas för kravnivå medel.

Funktionskrav KI5-3

Krav-id	Kravbeskrivning	Anmärkning
KI5-3-1	Systemet skall kunna upptäcka och hantera slumpmässiga fel i överföring och lagring.	
KI5-3-2	Systemet skall med mycket hög sannolikhet upptäcka och hantera försök till obehörig modifiering.	
KI5-3-3	Integritetsskyddet (t ex algoritmer, nyckelhantering, slumptalsgenerering, protokoll) skall ur kryptologiskt hänseende vara godkänt av TSA.	
KI5-3-4	Nycklar och certifikat tillverkade av TSA, eller på ett av TSA godkänt sätt, skall användas.	
KI5-3-5	Nycklar skall kunna raderas och bytas med enkla rutiner.	
KI5-3-6	Nycklar och algoritmer skall skyddas mot obehörig åtkomst och manipulation minst lika väl som den information de kryptografiska mekanismerna avser att skydda.	

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

Assuranskrav KI5-4

Krav-id	Kravbeskrivning	Anmärkning
KI5-4-1	Följande dokumentation skall levereras till TSA: • Högnivåbeskrivning av det kryptologiska systemet. • Lågnivåbeskrivning av samtliga kryptografiska komponenter, mekanismer och protokoll. • Kryptoverifieringsplan som skall godkännas av TSA. Källkod för alla ingående komponenter. Undantag kan ges för icke säkerhetskritiska COTS-komponenter.	
KI5-4-2	TSA skall tilldelas en referens av systemets krypto-relaterade delar.	
KI5-4-3	Kryptoverifiering skall utföras av TSA. Detta innebär att ett komplett system måste göras tillgängligt för praktiska tester.	
KI5-4-4	Systemet skall vara säkerhetsgranskat av en oberoende instans. I granskningsrapporten skall ingå säkerhetsmålsättning, penetrationstester samt källkods-granskning av säkerhetskritiska komponenter. Fullständig granskningsrapport från säkerhets-granskningen skall delges TSA.	

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

Kravnivå hög

Följande krav måste vara uppfyllda för att ett system för integritetsskydd skall kunna godkännas för kravnivå hög.

Funktionskrav KI5-5

Krav-id	Kravbeskrivning	Anmärkning
KI5-5-1	Systemet skall kunna hantera slumpmässiga fel i överföring och lagring.	
KI5-5-2	Systemet skall upptäcka och hantera alla försök till obehörig modifiering.	
KI5-5-3	Integritetsskyddet (t ex algoritmer, nyckelhantering, slumptalsgenerering, protokoll) skall ur kryptologiskt hänseende vara godkänt av TSA.	
KI5-5-4	Nycklar och certifikat tillverkade av TSA, eller på ett av TSA godkänt sätt, skall användas.	
KI5-5-5	Nycklar skall kunna raderas och bytas med enkla rutiner.	
KI5-5-6	Implementering av algoritmer i hårdvarukrets skall eftersträvas.	
KI5-5-7	Nycklar eller motsvarande skall lagras på ett sådant sätt att det är omöjligt att komma åt dem utan att bryta upp kryptoapparat el dyl.	
KI5-5-8	Kryptoapparat eller motsvarande skall vara RÖS-godkänd enligt nivå U1. Särskild vikt läggs vid nyckelhantering.	
KI5-5-9	Nyckel för integritetsskydd skall inte användas till andra skyddsmekanismer, till exempel sekretesskydd. Om nyckelhärledningsmetod används i system som implementerar flera skyddsmekanismer skall denna metod godkännas av TSA.	

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2007-03-27

Bilaga 1
12 830: 65517

Assuranskrav KI5-6

Krav-id	Kravbeskrivning	Anmärkning
KI5-6-1	Följande dokumentation skall levereras till TSA: • Högnivåbeskrivning av det kryptologiska systemet. • Lågnivåbeskrivning av samtliga kryptografiska komponenter, mekanismer och protokoll. • Kryptoverifieringsplan, vilken skall vara godkänd av TSA. • Källkod för alla ingående komponenter. Undantag kan ges för icke säkerhetskritiska COTS-komponenter.	
KI5-6-2	TSA skall tilldelas en referens av systemets krypto-relaterade delar.	
KI5-6-3	Kryptoverifiering skall utföras av TSA. Detta innebär att ett komplett system måste göras tillgängligt för praktiska tester.	
KI5-6-4	Systemet skall vara säkerhetsgranskat av en av TSA godkänd oberoende instans motsvarande CC EAL4++, där utökningen består av penetrationstester och källkodsgranskning. Fullständig granskningsrapport från säkerhetsgranskningen skall delges TSA.	

Bilaga 5

Exempel på disposition och innehåll i handling för godkännande av signalskyddssystem

FÖRSVARSMA
HÖGKVARTERET

HKV beteckning
12 839:

Sändlista

Ert tjänsteställe, handläggare	Ert datum	Er beteckning
Vårt tjänsteställe, handläggare	Vårt föregående datum	Vår föregående beteckning

Godkännande av signalskyddssystem XXX

Allmänt

Signalskyddssystem XXX (Maskinkrypto gemensamt typ X) omfattar följande komponenter:

Krypteringsapparat XXX (Kryapp XXX)

<Förrådsbenämning och beteckning på ingående delar>

<Typ av kryptonycklar>

<Benämning och beteckning på instruktion för hantering och användning>

< Upplysningar om instruktionen, tilldelning mm>

(Finns inte fastställd instruktion bör provisorisk instruktion bifogas denna skrivelse)

Beskrivning

<Allmän beskrivning av signalskyddssystemet>

Användning

<Beskrivning av användningsområde, syfte med systemet samt eventuella bestämmelser som är kopplade till användningen>

Restriktioner

<Bestämmelser för och beskrivning av eventuella restriktioner>

Underlag för godkännande

<Listning av samtliga dokument som skall ligga till grund för godkännandet. Av listan skall framgå utgivarens namn, dokumentdatum, ärendemening, KMÄ-nr eller motsvarande>

Följande dokument ligger till grund för godkännande:

<Dokument som skall listas>

Postadress	Besöksadress	Telefon	Telefax	E –post, Internet
107 85 Stockholm	Lidingövägen 24	08-788 75 00	08-788 77 78	exp-hkv@mil.se www.hkv.mil.se

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
20xx-xx-xx

HKV beteckning
12 839:

<TTEM> (finns inte TTEM skall uppdragsdokument motsv. anges)

<Kryptoverifiering>

<RÖS-mätning>

<Säkerhetsgranskningsrapport eller motsvarande>

<FMV typgodkännande> (typgodkännandet skall ta upp avvikelser från TTEM)

<Modifieringsdokumentation> (vid godkännande efter modifiering)

<Underhållsplan> (om möjligt)

<Övriga relevanta dokument>

Säkerhetsskydd

<Allmänna bestämmelser för säkerhetsskydd avseende b l a plombering av och åverkan på utrustning samt regler för hantering vid försändning och förrådställning>

Förvaring

<Bestämmelser för förvaring av materielen>

Försändning

<Bestämmelser för försändning av materiel>

Materielincident

<Bestämmelser för materielincidenter t ex förlust av materiel>

Utbildning

<Allmänt om utbildning>

Utbildning av systemoperatörer

<Bestämmelser för utbildning av systemoperatörer>

Utbildning av användare

<Bestämmelser för utbildning av användare>

Utbildning av underhållspersonal

<Bestämmelser för utbildningen av underhållspersonal såsom tekniker och/eller installatörer>

Redovisning

<Bestämmelser för redovisning av materielen>

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
20xx-xx-xx

HKV beteckning
12 839:

Sida 3 (4)

Underhåll och teknisk support

<Bestämmelser för underhåll>

Garantihantering

<Bestämmelser för garantihantering>

Teknisk support

<Bestämmelser för teknisk support, rörande installation, drift och underhåll>

Kryptonycklar

<Allmänt om kryptonycklar; typ, produktion, inläsning mm>

Nyckelserier

<Allmänna ej hemliga uppgifter om nyckelserier; fastställande, tilldelning, beställning, distribution samt i förekommande fall hänvisning till aktuell tilldelnings- och/eller driftsättningsskrivelse för nyckelserier>

Aktiva kort

<Uppgifter om vilka aktiva kort som stöds samt hänvisning till gällande regelverk för dessa)

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
20xx-xx-xx

HKV beteckning
12 839:

Beslut

Signalskyddssystemet XXX godkänns för användning enligt vad som framgår av detta dokument. Beslutet har fattats med stöd av Försvarsmaktens föreskrifter om signalskyddstjänsten inom totalförsvaret (FFS 2005:2).

Detta beslut har fattats av NN. I den slutliga handläggningen har dessutom NN deltagit och som föredragande NN.

NN
Chef för .....

NN

Sändlista:

Bilaga 6

Denna bilaga riktar sig i första hand till Försvarsmaktens insatsförband. Informationen kan även användas i tillämpliga delar för civila myndigheter/enheter motsv.

Begränsad respektive total förstöring

Begränsad respektive total förstöring beordras av myndighets-/enhets- eller förbandschef.

Signalskyddschef ansvarar för att förstöring ständigt är förberedd. All signalskyddspersonal bör vara väl insatt i de förberedelser som vidtagits för att vid behov snabbt kunna förstöra kryptonycklar, signalskyddshandlingar och signalskyddsmateriel.

När omedelbar fara föreligger för att kryptonyckel, signalskyddshandling, signalskyddsmateriel eller förbandsregister skall falla i motståndarens händer, utförs med hänsyn till läget begränsad eller total förstöring.

Åtgärder vid order om begränsad förstöring

- Reservexemplar av kryptonycklar och förbandsregister förstörs, återstående samlas in och förvaras så att de snabbt kan förstöras.
- Signalskyddsutrustning som inte används nollställs.
- Reservexemplar av kryptosambandstablåer och signalskyddshandlingar som inte längre erfordras förstörs.
- Återstående signalskyddsmateriel, hemliga handlingar och tablåer som inte oundgängligen behövs för pågående eller kommande arbete, samlas in och förvaras så att de snabbt kan förstöras.

Åtgärder vid order om total förstöring

- Kryptonycklar och förbandsregister förstörs.
- Signalskyddsutrustningar nollställs och väsentliga delar förstörs enligt respektive instruktion för systemets handhavande.
- Kryptosambandstablåer samt övriga hemliga handlingar och arbetspapper förstörs.

- Vid signalkontrollgrupp förstörs signalkontrollhandlingar och uppgifter som lagrats på band, diskett, hårddisk eller annat lagringsmedium.

Vidtagna åtgärder vid begränsad och total förstöring rapporteras snarast till närmast högre chef.

Bilaga 7

Huvudsaklig omfattning av administrativ kontroll

Allmänt

Myndighetens/enhetens delgivning av innebörden i 2 § i Försvarsmaktens föreskrifter om signalskyddstjänsten (FFS 2005:2).

Dokumentation/signalskyddsinstruktion

Aktualitet och delgivning

Myndighetens/enhetens dokumentation för att säkerställa signalskyddet, avseende fastställande och delgivning till berörd personal, samt handlingarnas koppling till övriga motsvarande dokument.

Organisation och personal

Myndighetens/enhetens:

- Dokumentation av signalskyddets organisation.
- Förteckning över samtlig signalskyddsutbildad personal samt personalens uppgifter, behörighet, tidpunkt för genomgången signalskyddsutbildning samt var utbildningen genomfördes och vem som gav utbildningen.
- Dokumentation av rutiner för vidmakthållande av signalskyddspersonalens kunskaper.
- Dokumentation över vidtagna eller planlagda åtgärder för att säkerställa samverkan med enheter i närområdet avseende ett eventuellt samutnyttjande av personal, materiel m m.

Materiel

Myndighetens/enhetens:

- Förteckning över tilldelad signalskyddsmateriel, med uppgift om individnummer och förvaringsplats (rum, säkerhetsskåp eller motsvarande).
- Dokumentation över åtgärder vid behov av reparation eller ersättning av signalskyddsmateriel.

- Dokumentation av åtgärder vid upptäckt förlust av eller åverkan på signalskyddsutrustning eller plombering.
- Dokumentation av överenskommelser eller avtal för ev utlånad signalskyddsmateriel till myndighet/enhet som inte omfattas av FFS 2005:2.
- Dokumentation över hur ev utlånad signalskyddsmateriel återförs.

Kryptonycklar

Myndighetens/enhetens:

- Dokumentation av hur myndighetens/enhetens försörjning med kryptonycklar sker.
- Förteckning över tilldelade nyckelserier och var dessa förvaras samt möjligheten till signalskyddat samband med andra enheter.
- Dokumentation av rutiner för mottagning, extern och intern distribution, delgivning, förvaring och rutinmässig förstöring av kryptonycklar. Förslagsvis kan detta illustreras i form av ett flödesschema eller i punktform.
- Dokumentation över åtgärder vid nyckelincident.
- Dokumentation över principer för distribution av kryptonycklar och uppgift om åtgärder då kryptonycklar ej har kommit myndigheten/enheten tillhanda inom föreskriven tid.

Aktiva kort/mjuka certifikat

Myndighetens/enhetens:

- Dokumenterade rutiner för beställning, mottagning/registrering, förteckning över tilldelade aktiva kort/mjuka certifikat, distribution, delgivning, hantering, förvaring, återsändning/revokering/förstöring.

Internkontroll

Myndighetens/enhetens:

- Planläggning av internkontroll samt protokoll efter genomförda internkontroller. För mer information se bilaga 8.

Åtgärdskalender

Dokumentation över myndighetens/enhetens åtgärder inom signalskyddstjänsten som skall vidtas vid olika slag av beredskapshöjningar, alternativt när sådan dokumentation skall ske först under ett återtagandeskede.

Signalskyddstjänstens säkerhetsskydd

Myndighetens/enhetens:

- Tillträdesskydd för utrymmen avsedda för signalskyddsverksamhet.
- Dokumentation av och rutiner för delgivna kryptonycklar och aktiva kort. Registrering av kryptonycklarnas följesedel.
- Förvaring av tilldelade kryptonycklar.
- Rutiner för redovisning och inventering av tilldelade kryptonycklar.
- Dokumentation av samt resurser för rutinmässig förstöring av kryptonycklar. Destruktörens status och skick.
- Förvaring och placering av signalskyddsmateriel. Hanteras signalskyddsmaterielen olika om den har inlästa kryptonycklar eller inte? Kontrolleras plomberingarna regelbundet?
- Hantering och förvaring av aktiva kort och tillhörande handlingar.

Övrigt

Myndighetens/enhetens:

- Tillgång och aktualitet på erforderliga publikationer.
- Signalskyddsberedskap.

Bilaga 8

Internkontroll av signalskyddstjänsten

Exempel på omfattning av myndighets/enhets interna kontroll av signalskyddstjänsten

Dokumentation och signalskyddstjänstens säkerhetsskydd

Aktualitet och delgivning

- När har signalskyddsinstruktionen upprättats (datum)? Är den uppdaterad?
- Av vem och när har instruktionen fastställts?
- Senaste revidering av instruktionen (datum). Vilka förändringar i signalskyddet ger anledning till att revidera instruktionen?
- Hur och när har berörd signalskyddspersonal delgivits instruktionen?

Organisation och personal

- Är signalskyddets organisation dokumenterad?
- Finns förteckning över samtlig signalskyddsutbildad personal? Av förteckningen skall framgå givna behörigheter, omfattning av och tidpunkt för utbildningen samt kursanordnande skola/lärare/behörig utbildare?
- Finns en tydlig ansvarsfördelning inom enhetens signalskyddsorganisation så att den fungerar även vid ansvarig befattningshavares frånvaro?

Signalskyddsmateriel och publikationer

- Finns aktuell förteckning över tilldelad signalskyddsmateriel, inklusive individnummer? Senast uppdaterad?
- Av förteckningen skall framgå var materielen är placerad och förvarad (rumsnummer eller motsv och ev säkerhetsskåp).

- Är signalskyddsmaterielen fysiskt placerad/förvarad enligt gällande bestämmelser?
- Hur är tillträdesskyddet ordnat för utrymmen avsedda för signalskyddsverksamhet?
- Återfinns i instruktionen uppgift om vilka åtgärder som skall vidtas vid upptäckt av förlust eller åverkan på utrustning eller plombering?
- Återfinns i instruktionen uppgift om åtgärder när materiel behöver repareras/ersättas?
- Finns dokumentation över åtgärder vid ev materielincident (signalskyddsincident)?
- Finns aktuella publikationer tillgängliga?

Kryptonycklar

- Finns tilldelade nyckelserier förtecknade? (Används godkänt datorstöd för bearbetning av sekretessbelagda uppgifter rörande signalskydd vid myndigheten/enheten?)
- Finns uppgift om åtgärder då kryptonycklar ej kommit fram till myndigheten/enheten inom föreskriven tid?
- Finns dokumenterade rutiner för beställning, mottagning/registrering, distribution, delgivning/inläsning, förvaring och rutinmässig förstöring av kryptonycklar?
- Finns dokumentation över åtgärder vid ev nyckelincident (signalskyddsincident)?
- Status på utrustning för rutinmässig förstöring av kryptonycklar? Godkänd spånstorlek är 2 x 2 mm eller 1,2 x 15 mm. Är uppgift om destruktörens placering dokumenterad?
- Destruktör bör regelbundet smörjas och dess restprodukt kontrolleras. Vid bränning skall kontroll av askan ske så att hela eller delar av nyckeln ej kan återskapas.

Kryptosambandstablå

- Framgår av dokumentationen möjlighet till signalskyddat samband med samverkande enheter (kryptosambandstablå eller telefonkatalog)?

Aktiva kort, certifikat

- Finns dokumenterade rutiner för beställning, mottagning/registrering, förteckning över tilldelade aktiva kort/mjuka certifikat, distribution, delgivning, hantering, förvaring, återsändning/revokering/förstöring?

Åtgärdskalender

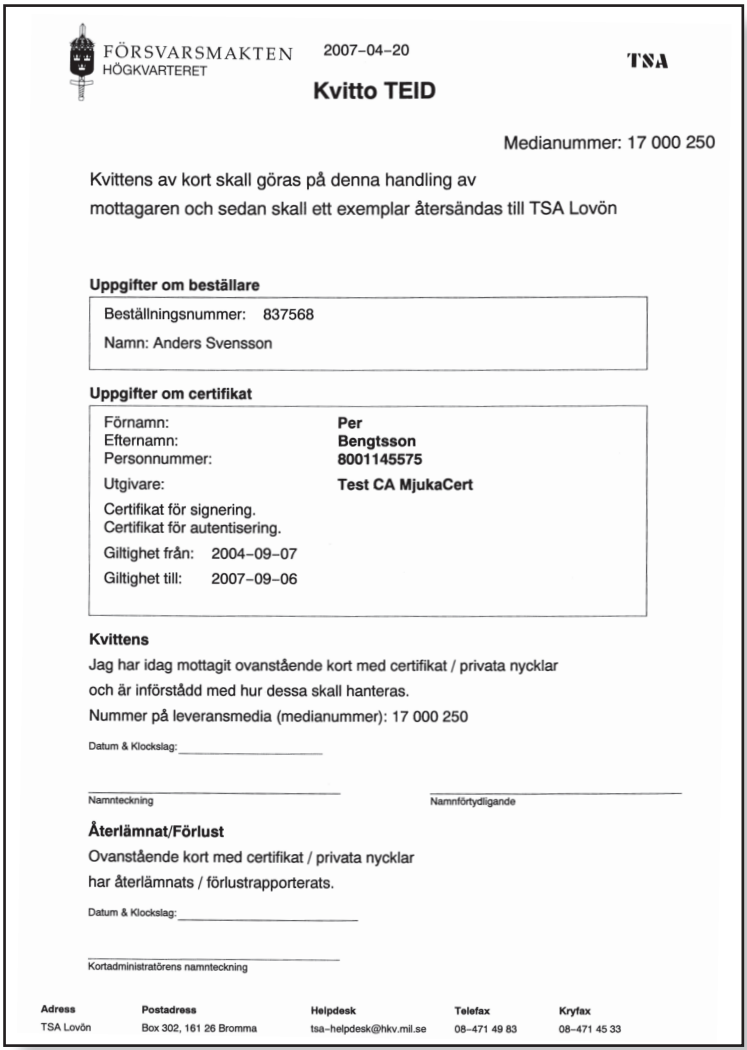
- Finns uppgift om vilka åtgärder som skall vidtas vid olika beredskapshöjningar?

Efter genomförd internkontroll

- Åtgärder efter internkontroll:
  - Vem åtgärdar ev påpekanden och upptäckta brister?
  - När skall de ev påpekandena och bristerna senast vara åtgärdade?
- Protokoll upprättas över genomförd internkontroll och sparas av myndigheten/enheten i minst tio år. Dokumentationen används som referens vid nästkommande internkontroll och vid administrativ kontroll genomförd av Högkvarteret TSA.
- Om internkontroll har skett vid en myndighets/enhets regionala eller lokala organisationsenhet bör protokollet även delges myndighetens/enhetens huvudkontor, stab, centrala ledning eller motsvarande.
- Planering av tidpunkt för nästkommande internkontroll

Bilaga 9

Exempel på kvitto för TEID och TAK



FÖRSVARSMAKTEN
HÖGKVARTERET

2007–04–20

TSA

Kvitto TEID

Medianummer: 17 000 250

Kvittens av kort skall göras på denna handling av
mottagaren och sedan skall ett exemplar återsändas till TSA Lovön

Uppgifter om beställare

Beställningsnummer: 837568
Namn: Anders Svensson

Uppgifter om certifikat

Förnamn:	**Per**
Efternamn:	**Bengtsson**
Personnummer:	**8001145575**
Utgivare:	**Test CA MjukaCert**

Certifikat för signering.
Certifikat för autentisering.

Giltighet från: 2004–09–07
Giltighet till: 2007–09–06

Kvittens

Jag har idag mottagit ovanstående kort med certifikat / privata nycklar
och är införstådd med hur dessa skall hanteras.
Nummer på leveransmedia (medianummer): 17 000 250

Datum & Klockslag: _____

_____ _____
Namnteckning Namnförtydligande

Återlämnat/Förlust

Ovanstående kort med certifikat / privata nycklar
har återlämnats / förlustrapporterats.

Datum & Klockslag: _____

_____
Kortadministratörens namnteckning

Adress	Postadress	Helpdesk	Telefax	Kryfax
TSA Lovön	Box 302, 161 26 Bromma	tsa–helpdesk@hkv.mil.se	08–471 49 83	08–471 45 33

Allmänna hanteringsregler

Certifikatinnehavare skall:

- Kontrollera att medianummer på CD/kort och datapost överensstämmer med angivet medianummer på de kvitton som medföljer (2 st).
- Kvittera CD/kort på medföljande kvitton (2 st).
- Anmäla eventuell förlust av CD/kort och/eller datapost till kortadministratören. Om kortadministratören inte finns tillgänglig skall förlustanmälan av CD/kort/datapost göras direkt till TSA Helpdesk.
- Vid avslutad anställning meddela kortadministratör detta.
- Vid byte av servercertifikatansvarig meddela kortadministratören detta samt lämna in CD, kvitto och datapost till kortadministratören för överlämnade till ny servercertifikatansvarig.

Hanteringsregler för mjukt certifikat avsett för öppen information

Certifikatinnehavare skall:

- Ansvara för att CD innehållande certifikat som upphört att gälla/revokerats förstörs.
- Ansvara för att datapost till certifikat förstörs när dessa har upphört att gälla/revokerats.

Hanteringsregler för CD stämplad SG R och TEID

Certifikatinnehavare skall:

- Förvara sitt exemplar av kvittot, datapost och TEID/CD så att obehörig ej kan komma åt innehållet.
- Ansvara för att CD stämplad **SGR** och/eller TEID som upphört att gälla eller revokerats återlämnas till kortadministratören.
- Ansvara för att datapost till certifikat förstörs när dessa har upphört att gälla.

FÖRSVARSMAKTEN
HÖGKVARTERET

2007-04-20

TSA

Kvitto TAK

Medianummer: 17 000 330

Kvittens av kort skall göras på denna handling av
mottagaren och sedan skall ett exemplar återsändas till TSA Lovön

Uppgifter om beställare

Beställningsnummer: AK2004-1-36-3
Namn: BÖRJE ANDERSSON

Uppgifter om certifikat

Förnamn:	**BÖRJE**
Efternamn:	**ANDERSSON**
Personnummer:	**4212256954**

Utgivare:

Certifikat för signering.
Certifikat för autentisering.

Giltighet från: 2004-09-07

Giltighet till: 2007-09-06

Kvittens

Jag har idag mottagit ovanstående kort med certifikat / privata nycklar
och är införstådd med hur dessa skall hanteras.
Nummer på leveransmedia (medianummer): 17 000 330

Datum & Klockslag: _____

_____ _____
Namnteckning Namnförtydligande

Återlämnat/Förlust

Ovanstående kort med certifikat / privata nycklar
har återlämnats / förlustrapporterats.

Datum & Klockslag: _____

_____
Kortadministratörens namnteckning

Adress	Postadress	Helpdesk	Telefax	Kryfax
TSA Lovön	Box 302, 161 26 Bromma	tsa-helpdesk@hkv.mil.se	08-471 49 83	08-471 45 33

Hanteringsregler för servercertifikatansvarig och/eller användare

Servercertifikatansvarig eller användare skall, vad avser aktiva kort och certifikat:

- Efter kvittens, ständigt ha kontroll över sitt aktiva kort/CD samt följa övriga regler för hantering av kort, kvitton, datapost och koder.
- Förvara sitt exemplar av kvittot, datapost och aktivt kort/CD så att obehörig ej kan komma åt innehållet.
- Kontrollera att medianummer på kort/CD och datapost överensstämmer med angivet medianummer på de kvitton som medföljer (2 st).
- Kvittera kort/CD på medföljande kvitton (2 st).
- Anmäla eventuell förlust av CD/kort och/eller datapost till kortadministratören. Om kortadministratören inte finns tillgänglig skall förlustanmälan av CD/kort/datapost göras direkt till TSA Lovön, HELPDESK.
- Vid avslutad anställning återlämna CD/aktivt kort till den lokala kortadministratören samt övervaka att anteckning på att CD:n/kortet är återlämnat görs på tillhörande kvitto.
- Ansvara för att CD/aktivt kort som upphört att gälla återlämnas till kortadministratören.
- Vid avslutad anställning meddela kortadministratör detta.

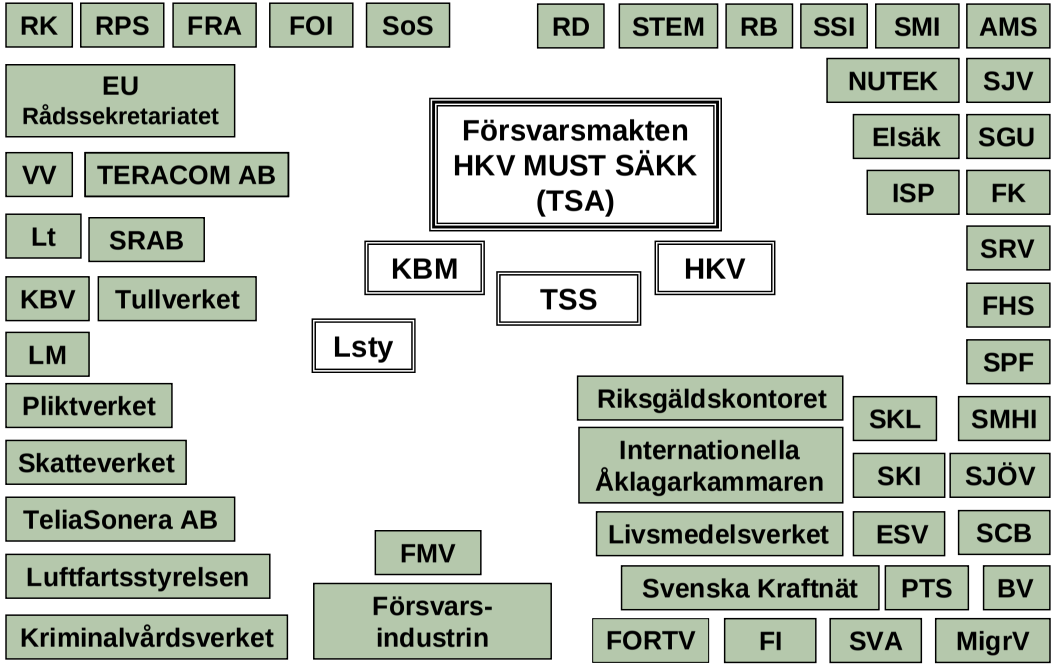
Användare av aktiva kort skall:

- Radera inlästa kryptonycklar på kortet när de upphört att gälla.
- Vid felaktigt eller skadat aktivt kort anmäla detta till lokal kortadministratör
- Vid återlämning av TAK spärra sitt kort genom att ange felaktig PUK ANV och PUK KRY tre på varandra följande gånger.
- Vid ankomst till ny tjänstgöringsplats ”registrera” sitt aktiva kort hos den nya kortadministratören.

Servercertifikatansvarig skall:

- Vid byte av servercertifikatansvarig meddela kortadministratören detta samt lämna in CD, kvitto och datapost till kortadministratören för överlämnande till ny servercertifikatansvarig.

Myndigheter/enheter samt vissa företag som bedriver signalskydds-verksamhet i någon form - den s k ”signalskyddsfamil□en”



AMS	Arbetsmarknadsstyrelsen
BV	Banverket
ELSÄK	Elsäkerhetsverket
STEM	Statens Energimyndighet
ESV	Ekonomistyrningsverket
FHS	Försvarshögskolan
FI	Finansinspektionen
FMV	Försvarets materielverk
FOI	Totalförsvarets forskningsinstitut
FORTV	Fortifikationsverket
FRA	Försvarets radioanstalt
HKV	Försvarsmaktens högkvarter
ISP	Inspektionen för strategiska produkter
KBM	Krisberedskapsmyndigheten
KBV	Kustbevakningen
LM	Lantmäteriet
Lsty	Länsstyrelse
Lt	Landsting
MigrV	Migrationsverket
MUST	Militära underrättelse- och säkerhetstjänsten
NUTEK	Verket för näringslivsutveckling
PTS	Post- och Telestyrelsen
RB	Sveriges riksbank
RD	riksdagen
FK	Försäkringskassan
RK	regeringskansliet
RPS	Rikspolisstyrelsen

SCB	Statistiska centralbyrån
SGU	Sveriges geologiska undersökning
SJV	Statens jordbruksverk
SJÖV	Sjöfartsverket
SKI	Statens kärnkraftsinspektion
SKL	Statens Kriminaltekniska Laboratorium
SMHI	Statens meteorologiska och hydrologiska institut
SMI	Smittskyddsinstitutet
SoS	Socialstyrelsen
SPF	Styrelsen för psykologiskt försvar
SRAB	Sveriges Radio AB
SRV	Statens räddningsverk
SSI	Statens strålskyddsinstitut
SVA	Statens veterinärmedicinska anstalt
SÄKK	Säkerhetskontoret
TSA	Funktionen för totalförsvarets signalskyddssamordning
TSS	Totalförsvarets signalskyddsskola
VV	Vägverket

Bilaga 11. Begrepp inom signalskyddstjänsten

Aktiva kort	Utöver de aktiva korten TAK, TEID och NBK finns även databärarkort (DBK) avsett för lagring av data samt nyckelbärarkort av äldre typ (TAK/NBK) som används för att hantera kryptonycklar för äldre system.
Anropsnyckel	Förteckning över registernummer och rörliga anropssignaler som svarar mot dessa.
Anropssignal	Reglementerad signal för adressering och dirigering av signalmeddelande. Sådan signal kan användas för angivande/identifiering av enhet. Se rörlig anropssignal, fast anropssignal och tillfällig anropssignal.
Anropssignalsystem	Medel och metod för adressering och dirigering av signalmeddelande.
Användare av signalskyddssystem	Person som i telekommunikations- och IT-system, där signalskydd ingår, är behörig att handha signalskyddsmateriel och/eller kryptonycklar.
Asymmetriskt krypto	Kryptografiskt system där olika nycklar används för kryptering och dekryptering. Den ena nyckeln är privat och den andra nyckeln är publik. Se även RSA.
Autentisering	Kontroll av uppgiven identitet, t ex vid inloggning.

Bandspridning	Metod för att sprida en sändares effekt över ett brett frekvensspektrum för att försvåra upptäckt av sändande enhet och minska verkan av smalbandig störning.
Behörig befattningshavare	*Inom signalskyddstjänsten:* Befattningshavare som behöver ifrågavarande uppgifter för sin tjänst och som har genomgått säkerhetsprövning samt erforderlig signalskydds- och säkerhetsutbildning.
Behörighetskontroll	Administrativa och tekniska åtgärder för kontroll av användares identitet, styrning av användares behörighet att använda systemet och dess resurser samt för registrering av denna användare.
Beredskapsnyckel	Kryptonyckel som används under höjd beredskap.
Biträdande signalskyddschef	Särskilt signalskyddsutbildad person som biträder signalskyddschefen med ledning av signalskyddstjänsten.
Blandad text	Text sammansatt av täcktermer eller omskrivningar och klartext. Text som består av enbart täcktermer räknas också till blandad text.
Blockerat kort	Aktivt kort där användarens PIN angivits felaktigt tre gånger.
Central katalogtjänst	Katalog där systemansvariga/användare kan hämta certifikat och revokeringslistor.
Certifiering	Formellt fastställande av resultat från en evaluering (se evaluering).
Certifikat	Användarens publika RSA-nyckel tillsammans med dennes namn och annan information signerad av certifikatutfärdaren.

Certifikatpolicy Certificate Policy (CP)	Publikt policydokument som beskriver det ansvar och ändamål som certifikatutfärdaren intygar för beträffande sin verksamhet.
Certificate Practice Statement (CPS)	Regelverk som certifikatutfärdaren åtar sig att följa i sin verksamhet.
Certifikatutgivare Certification Authority (CA)	Betrodd instans som har till uppgift att skapa och utge certifikat.
Certifikatutgivarens signatur	Data signerad med utgivarens privata RSA-nyckel som garanterar ett certifikats äkthet.
Chiffer	Kryptosystem av nedanstående slag: • Utbyteschiffer; klartextens tecken byts ut mot andra tecken enskilt eller gruppvis. Till utbyteschiffer räknas dock icke kod. • Omkastningschiffer; ordningsföljden mellan klartextens tecken kastas om.
CIRK-nyckel	Kryptonyckel avsedd för krypto-samband från en bestämd avsändare till flera bestämda mottagare.
Datapost	Handling innehållande PIN, PUK för aktivt kort eller lösenord för mjukt certifikat.
Dekryptera	Återföra kryptotext till klartext med hjälp av använt kryptosystem.
Delsträckskryptering	Kryptering på varje delsträcka för sig.
Digital signatur	Kryptografisk omvandling av ett meddelande på ett sätt som endast avsändaren kan utföra och som tillåter mottagaren att kontrollera meddelandets äkthet, innehåll och avsändarens identitet.

Direktsekvens	Metod för bandspridning där den digitala datasignalen sprids över frekvensbandet genom att moduleras med en mycket hög pseudoslumpfrekvens.
Distributionsenhet	Enhet som ansvarar för distribution av kryptonycklar.
Engångschiffer	Utbyteschiffer i vilket kryptering utförs med hjälp av en för varje meddelande unik nyckel (blankett) på ett sådant sätt att varje klartexttecken krypteras med ett tecken ur nyckeln. Rätt använt är engångschiffer oforcerbart.
Engångskod	Kod där kryptering och dekryptering utförs med hjälp av speciellt utformade kodord som endast får användas en gång.
Enhetsförpackning	Förpackning som innehåller en enhets första behov av beredskapsnycklar.
Ersättningsnyckel	Kryptonyckel som har producerats och distribuerats i förväg och som är avsedd att ersätta ordinarie kryptonyckel.
Evaluering	Säkerhetsteknisk utvärdering av ett system eller en systemkomponent.
F/B-nyckel	*Freds-/Beredskapsnyckel:* kryptonyckel som används under grundberedskap och höjd beredskap.
Falsk signalering	Försåtlig inblandning i signalering för att t ex skapa förvirring, blockera kommunikationen eller inhämta underrättelser.
Falsk kommunikation	Se falsk signalering.
Fast anropssignal	Anropssignal som normalt inte byts.
Fast frekvens	Frekvens som normalt inte byts annat än av trafikala skäl, t ex vid övergång från dag- till nattfrekvens.

Fingerat kryptomeddelande	Meddelande med samma utseende som ett kryptomeddelande men som inte är avsett att dekrypteras.
Flerkanalkryptering	Kryptering av flera samtidiga transmissionskanaler multiplexerade till en kanalgrupp.
Forcering	Se nyckelforcering och textforcering.
Fredsnyckel	Kryptonyckel som används under grundberedskap.
Frekvenshopp	Metod för bandspridning där frekvensen byts efter ett pseudoslumpmässigt mönster.
Funktionsspecifikt signalskyddssystem	Signalskyddssystem som anskaffats för en viss funktion och som inte är gemensamt. (se även gemensamt signalskyddssystem).
Fyllnadssignalering	Signalering inom ordinarie signalnät för att utjämna röjande variationer i trafikvolymen eller för att skapa oregelbundet återkommande trafiktoppar bland vilka de verkliga topparna skall kunna döljas.
Förbandsregister	Förteckning över registernummer och identitetsuppgifter för enheter som skall anges med rörliga anropssignaler. Förbandsregister finns som ordinarie och ersättningsalternativ.
Förberedda kort	Aktivt kort som förses med data utan koppling till person eller roll, detta som förberedelse för senare personalisering.
Försvarsmakten närstående myndigheter	Försvarets materielverk (FMV), Försvarets radioanstalt (FRA), Försvarshögskolan (FHS), Totalförsvarets forskningsinstitut (FOI), Totalförsvarets pliktverk (PliktV) och Fortifikationsverket (FORTV)

Försvarssekretess	Sekretess för uppgift som angår verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt utgör fara för rikets säkerhet om uppgiften röjs. Kan även benämnas totalförsvarssekretess.
Gemensamt signalskyddssystem	Signalskyddssystem som anskaffats för att användas i två eller flera funktioner inom totalförsvaret.
Grundhandling TAK	Redovisningshandling för äldre TAK (generation 1) som under kortets giltighetstid förvaras av lokal kortadministratör.
Incident med aktivt kort/ mjukt certifikat	När obehörig har fått tillgång till aktivt kort med certifikat/privat nyckel eller mjukt certifikat eller dess koder/lösenord.
Informationsoperation	Med informationsoperationer koordineras verkan på informationsarenan genom att påverka data och information i syfte att påverka motståndarens eller andra aktörers agerande, samtidigt som egen verksamhet på informationsarenan skyddas.
Informationssäkerhetsklass	Med informationssäkerhetsklass avses i denna handbok detsamma som anges i 4 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd. Informationssäkerhetsklass innebär en indelning av Försvarsmaktens säkerhetsskydd i någon av följande fyra informationssäkerhetsklasser: HEMLIG/TOP SECRET, HEMLIG/SECRET, HEMLIG/CONFIDENTIAL och HEMLIG/RESTRICTED.

Inre nyckel	Se kryptonyckel.
Internt kabelnät	Kabelbaserat telenät som inte är anslutet till publika telenät.
IS UNDSÄK TSA	Delsystem i Försvarsmaktens informationssystem UNDSÄK som stödjer beställning, produktion, och redovisning av aktiva kort, certifikat och kryptonycklar.
Klartext	Text, bild, data eller tal utformat på sådant sätt att innebörden kan förstås. Till klartext räknas förutom fullständiga ord, vilkas innebörd kan förutsättas allmänt kända, även allmänt brukliga förkortningar, förkortningar som används i svenskt eller internationellt fackspråk, koder för offentligt bruk samt lägesbeteckningar enligt Rikets nät, Georef eller UTM.
Kodord	Överenskommet uttalbart ord som används för att dölja förutsedd order, orientering, rapport eller händelse.
Kompletteringstabell	Tabell som innehåller aktuella klartextuttryck (förband, orter, verksamhet m m) för komplettering av täcktabell.
Kortadministratör	Person som ansvarar för beställning, utlämning, upplåsning m m samt redovisning av aktiva kort och mjuka certifikat inom eget ansvarsområde.
Kortanvändare	Person som är behörig att använda aktivt kort.
Kortförpackning	Förpackning innehållande aktiva kort. Förpackningen kan utgöras av påse tillverkad av ogenomskinlig plast.
Kortinnehavare	Person som kvitterat aktivt kort.
Kortterminal/Kortläsare	Utrustning för att kommunicera med ett aktivt kort.

Kortutgivare	Betrodd instans som utför personalisering, d v s förser ett aktivt korts integrerade krets med data för att kortet skall bli användbart.
Kryptera	Omvandla klartext till kryptotext med hjälp av kryptosystem.
Krypteringsapparat	Utrustning avsedd för kryptering och dekryptering. Kan även benämnas kryptoapparat eller kryapp.
Kryptoalgoritm	Schema för omvandling av klartext till kryptotext.
Kryptobeteckning (krybet)	Teckengrupp som i kodad form anger en nyckels system- och serietillhörighet samt lottningsnummer.
Kryptomassa	Följd av tecken som ser ut som kryptotext och som används vid övnings- och fyllnadssignalering.
Kryptomateriel	Se signalskyddsmateriel.
Kryptomodul	Elektronisk komponent som kan kryptera och dekryptera.
Kryptonyckel	1. Data (inre nyckel), som tillsammans med yttre nyckel, inom ett signalskyddssystems ram, reglerar hur klartext omvandlas till kryptotext, blandad text, frekvensval i frekvenshoppsystem eller hur anropssignal eller lösen skall utformas. 2. Informationsbärare av vilken framgår data enligt 1 ovan för angivet signalskyddssystem. 3. Definition enligt 3 § FFS 2005:2.
Kryptosamband	Möjlighet att överföra krypterad information.

Kryptosambandstablå	Sammanställning av enheters möjlighet att med hjälp av signalskyddssystem och nyckelserier överföra krypterad information med samverkande myndigheter/enheter.
Kryptosystem	Se definition av signalskyddssystem.
Kryptotext	Data som genom kryptering bildas ur klartext i avsikt att dölja innehållet för obehöriga.
Kryptotjänstmeddelande	Tjänstemeddelande rörande krypteringsarbete.
Leveranslösenord	Slumpsträng som används för att kryptera användarens privata nyckel vid leverans från CA.
Lottningsnummer	LO-NR. Nummer på kryptonyckel som upplyser användaren om i vilken ordning respektive nyckel i en serie skall tas i bruk.
Lösen	Ord, tecken eller signal som används för kontroll av behörighet.
Lösennyckel	(Krypto)nyckel som används vid lösensignalering.
Lösensignalering	Metod för behörighetskontroll genom utväxling av lösen vid signalering.
Lösensystem	Medel och metod för behörighets-kontroll vid signalering.
Maskerande signalering	Signalering med avsikt att dölja underrättelsegivande signalering i annan signalering.
Materielincident	När signalskyddsmateriel saknas eller kan antas ha manipulerats.
Meddelandenyckel	Se yttre nyckel.
Mjukt certifikat	Privat nyckel och certifikat lagrat på fil.

Motringning	Metod för behörighetskontroll. Den uppringde avbryter telefonsamtalet och ringer efter kontroll i sin tur upp (motringer) den uppringande.
Mottelefonering	Se motringning.
NBK	Totalförsvarets nyckelbärarkort. Se nyckelbärarkort.
NCSA (National Communications Security Authority)	Den organisation i ett land som verifierar och godkänner krypton. Regeringen utser den myndighet som skall inneha NCSA-rollen.
NDA (National Distribution Authority)	Den organisation i ett land som genererar och distribuerar kryptonycklar.
Nyckeladministratör	Person som administrerar kryptonycklar enligt signalskyddschefens bestämmande.
Nyckelbärarkort (NBK)	Aktivt kort avsett som bärare av data och kryptonycklar.
Nyckelincident	När en kryptonyckel eller dess nyckelinformation bedöms ha eller har kommit till obehörigs kännedom.
Nyckelforcering	Rekonstruktion av en använd nyckel när kryptosystem och kryptotext är kända samt eventuellt även klartexten.
Nyckelförpackning	Förpackning innehållande kryptonycklar för visst signalskyddssystem och viss nyckelserie för en viss period. Förpackningen kan utgöras av påse tillverkad av ogenomskinlig plast.
Nyckelinformation	De data som inom ett signalskyddssystems ram reglerar hur klartext omvandlas till kryptotext.
Nyckelinjektor	Elektroniskt minne för säker lagring och transport av kryptonycklar samt för inläsning av dessa i signalskyddsutrustning.

Nyckelserie	Kryptonycklar avsedda för ett visst användningsområde.
Omskrivning	Omvandling av klartext till blandad text genom hänvisning till handling, händelse, sakförhållande, som meddelandets mottagare men inte obehörig känner till.
Periodförpackning	Förpackning innehållande en nyckelförpackning av varje tilldelad nyckelserie för ett visst antal dygns behov.
Personaliserat kort	Aktivt kort försett med data knutet till en viss person eller roll.
Personalisering	Process där kort-, kortutgivar- och kortinnehavarspecifika kataloger och datafiler skapas och skrivs in i det aktiva kortet. Personaliseringen kan delas upp i flera steg.
Personlig identifieringskod (PIN)	Se PIN.
PIN (Personal Identification Number)	*Personlig identifieringskod:* lösenord oftast bestående av enbart siffror.
PIN ADM	Kortadministratörs-PIN som möjliggör byte av certifikat och personalisering av förberett kort.
PIN ANV	Kortanvändarens PIN som möjliggör användning av autentiseringsnyckeln.
PIN KRY	Kortanvändarens PIN som möjliggör lagring och läsning av kryptonycklar.
PIN SIGN	Kortanvändarens PIN som möjliggör användning av signeringsnyckeln samt administration av fingeravtryck.
Privat RSA-nyckel	Privat nyckel som används vid generering av digital signatur, vid autentisering samt vid dekryptering.

Provsändning	Med provsändning avses: *Funktionsprov:* Anläggningsvis sändning vid leverans, tillsyn eller översyn med tidsintervall enligt tidsplan. *Systemprov:* Anläggningsvis sändning, med fler än ett delsystem.
PTP-nyckel	*Punkt till punkt nyckel:* kryptonyckel enbart avsedd för kryptosamband mellan två bestämda enheter.
Publik RSA-nyckel	Publik nyckel som görs allmänt känd i ett certifikat och som används vid verifiering av digitala signaturer, vid autentisering samt vid kryptering.
PUK (Personal Unblocking Key)	*Personlig upplåsningskod:* Används till att låsa upp en blockerad PIN.
Radiolänk	Radioutrustning för riktat samband som kan ske över en kedja av relästationer.
Radiotystnad	Fullständigt eller begränsat förbud att använda radio- och radiolänksändare.
Registerkontroll	Inhämtning av uppgifter från polisregister i samband med säkerhetsprövning av en person (se säkerhetsprövning).
Revokerat certifikat	Certifikat som återkallats innan dess giltighetstid har gått ut.
Revokeringslista (CRL – Certificate Revocation List)	Periodiskt uppdaterad, tidsstämplad och signerad lista, utgiven av certifikatutfärdaren, över certifikat som återkallats innan deras giltighetstid har gått ut. Kallas ibland spärrlista.
Rollkort	Aktivt kort som på förhand utfärdas för en viss befattning eller funktion.

RSA	Kryptografiskt system där olika nycklar används för kryptering och dekryptering. Den ena nyckeln är privat och den andra nyckeln är publik. RSA används också för autentisering och för att skapa digitala signaturer. Upphovsmännen **R**ivest, **S**hamir och **A**dleman har givit systemet dess namn.
Röjande signaler (RÖS)	Icke önskvärda elektromagnetiska och/eller akustiska signaler, som alstras i informationsbehandlande utrustningar och som kan bidra till att sekretessbelagd information röjs, om de kan tydas av obehörig.
Röjd kryptonyckel	Se nyckelincident.
Rörlig anropssignal	Anropssignal som byts efter bestämda regler för att försvåra för obehörig att identifiera enhet eller förbindelse.
Rörlig frekvens	Frekvens som byts efter bestämda regler för att försvåra för obehörig att upptäcka eller identifiera sändande enhet.
Signaldisciplin	Innebär att fastställd terminologi används och att gällande sändnings- och signalskyddsrutiner följs.
Signalkontroll	Förutom det som beskrivs under avsnittet ”Definitioner” syftar signalkontroll även till att försvåra eller om möjligt förhindra främmande signalunderrättelsetjänst eller annan obehörigs inriktning mot, åtkomst, störande eller manipulering av information i våra telekommunikations- och IT-system.
Signalskydd	Åtgärder som syftar till att förhindra obehörig insyn i och påverkan av vårt lands telekommunikationer samt användning av kryptografiska funktioner i IT-system.

Signalskyddsbedömande	Klarläggande av aktuellt telehot och egna möjligheter att genom signalskyddsåtgärder minska verkan av motståndarens telekrigföring.
Signalskyddsbefattning	Till signalskyddsbefattning räknas: signalskyddschef, biträdande signalskyddschef, systemoperatör, nyckeladministratör och kortadministratör.
Signalskyddschef	Person som har till uppgift att ansvara för ledning och samordning av signalskyddstjänsten.
Signalskyddsgrad (SG)	Anger signalskyddssystemets styrka.
	Används vid märkning av kryptonycklar för att ange vilken signalskyddsgrad en viss nyckelserie är godkänd för.
	Ger vägledning vid hantering av kryptonycklar.
Signalskyddsincident	Omfattar nyckelincident, materielincident samt incident för aktivt kort/mjukt certifikat.
Signalskyddsinstruktion	Handling som bl a redovisar en myndighets eller enhets planläggning och organisation av signalskydds-tjänsten.
Signalskyddskontroll	Kontroll av att signalskyddssystem fungerar och handhas på ett korrekt sätt.
Signalskyddsläge	Sammanfattande benämning på resurser och handlingsmöjligheter utifrån materiel- och personalläge för signalskyddstjänsten.
Signalskyddslärare	Person som är behörig att utbilda i grund- och systemutbildning i signalskydd.
Signalskyddspersonal	Personal placerad i signalskyddsbefattning (se signalskyddsbefattning).

Signalspaning	Del i signalunderrättelseprocessen med fokus på inhämtning av signaler. Se även signalunderrättelsetjänst.
Signaltjänstkontroll	Kontroll av att signalering utförs enligt gällande regler.
Signalunderrättelsetjänst	Omfattar inhämtning, bearbetning, analys och rapportering av signaler. Signalunderrättelsetjänst är ett vidare begrepp än signalspaning och motsvaras i internationella sammanhang av begreppet ”Signal Intelligence” (Sigint).
Snabbsändning	Sändning med sändningstid som understiger en sekund.
Spärrat kort	Aktivt kort där felaktig upplåsningskod för användarens PIN angivits tre gånger i följd så att kortet blivit oanvändbart.
Störsändning	Sändning i avsikt att hindra eller försvåra användning av teletekniska medel.
Symmetriskt krypto	Kryptografiskt system där likadana nycklar används för kryptering och dekryptering av klartext respektive kryptotext.
Systemadministratör	Person som är ansvarig för driften av ett IT-system.
Systembestämmelse	Se systeminstruktion.
Systeminstruktion	Instruktion som reglerar användning och handhavande av ett signalskyddssystem.
Systemnyckel	Kryptonyckel som preciserar arbetssättet hos en krypteringsapparat.
Systemoperatör	Person med särskild signalskyddsutbildning som handhar signalskyddsmateriel och kryptonycklar för ett eller flera signalskyddssystem.

Säkerhetsprövning	Bedömning av uppgifter som belyser en persons lämplighet för anställning eller deltagande i verksamhet som har betydelse för rikets säkerhet m m, enligt säkerhetsskyddslagen. (SFS 1996:627) Underlag för säkerhetsprövning är personlig kännedom om den prövade, betyg, intyg, referenser, registerkontroll och särskild personutredning m m, enligt säkerhetsskyddsförordningen. (SFS 1996:633)
TAK	**T**otalförsvarets **A**ktiva **K**ort. Se Totalförsvarets aktiva kort.
TEID	**T**otalförsvarets **E**lektroniska **ID**-kort. Se Totalförsvarets elektroniska ID-kort
Telehot	Art och omfattning av väntad telekrigföringsinsats.
Teleskydd	Åtgärder för att minska verkan av telekrigföring. Teleskydd för signalering kallas signalskydd.
Testnyckel	Nyckel som används för funktionstest av krypteringsapparat och kryptosamband. Testnyckel ger inget signalskydd.
Textforcering	Rekonstruktion av en klartext med kännedom om kryptosystem och kryptotext men utan tillgång till använd nyckel.
Textskydd	Signalskyddsåtgärder som syftar till att hindra eller försvåra för obehörig att tyda överförd eller lagrad information. Textskydd åstadkoms genom kryptering eller omskrivning.
Tillfällig anropssignal	Fast eller rörlig anropssignal som väljs ut bland ej utnyttjade anropssignaler i visst anropssignalsystem (viss anropsnyckel) för att tillfälligt ange enhet.

Tillfällig lägesangivningstabell	Tabell med koordinater som används för att vid ett bestämt tillfälle dölja uppgift om geografiskt läge.
Tillfällig verksamhetstabell	Tabell med täcktermer som används för att täcka texten till meddelanden av SG R, exempelvis TIVETA.
Tillfällig övningsnyckel (TIFÖ-nyckel)	Kryptonyckel som används vid större tillämpade övningar.
Tolka	Återföra blandad text till klartext med hjälp av täcktabell och gällande täcknyckel, tillfälligt lägesangivningssystem eller tillfällig verksamhetstabell.
Totalförsvaret	Totalförsvaret består av militär verksamhet (militärt försvar) och civil verksamhet (civilt försvar).
Totalförsvarets aktiva kort (TAK)	Aktivt kort framtaget för totalförsvaret, avsett för identifiering av användare, signering av information samt som bärare av data och kryptonycklar.
Totalförsvarets Elektroniska ID-kort (TEID)	Aktivt kort framtaget för totalförsvaret, avsett för identifiering av användare, signering av information samt som bärare av data och kryptonycklar avsedda för signalskyddsgrad SG R.
Totalsträckskryptering (End-to-end encryption)	Meddelande krypteras där information genereras, transporteras och dekrypteras först hos mottagaren.
Trafikanalys	Undersökning av trafikflöden i ett kommunikationsnät för att erhålla uppgifter om trafikintensitet, meddelandelängder, avsändar- och mottagaradresser i syfte att erhålla underrättelser t ex om ledningsförhållanden, styrka, gruppering, verksamhet och avsikt.

Trafikansvarig	Myndighet eller enhet som för visst radio- eller telenät ansvarar för trafikregler och instruktioner, detaljplanläggning i övrigt och samordning i detalj med övriga nät.
Trafikflödesskydd	Skydd mot trafikanalys som syftar till att maskera att information förekommer dels genom att all information på en teleförbindelse krypteras, dels genom att pauser i informationsbytet fylls ut med äkta eller simulerad kryptotext.
Trafiklista	Ifylld trafiklista/uppföljningslista används som underlag för menbedömning vid nyckelincident och bör därför sparas i minst 1 år. Trafiklista kan användas för de flesta signalskyddssystem och bör innehålla uppgifter om tidpunkt, adressater, avsändare, ärendemening samt kryptobeteckning vid sändning av ett krypterat meddelande eller genomförande av ett krypterat samtal.
Trafikskydd	Signalskyddsåtgärder som syftar till att hindra eller försvåra för obehörig att upptäcka och avlyssna eller pejla vår radio- och telekommunikation, hindra eller försvåra trafikanalys, minska verkan av störsändning samt hindra eller minska verkan av falsk signalering.
Täcka	Omvandla klartext till blandad text med hjälp av täcktabell och gällande täcknyckel, tillfälligt lägesangivningssystem eller tillfällig verksamhetstabell.
Täcknyckel	Se kryptonyckel.
Täcksystem	Medel och metod för täckning och tolkning.

Täcktabell	Tabell med vars hjälp klartext omvandlas till blandad text.
Upplåsningskod (PUK)	Se PUK.
Utbildningskort	Aktiva kort endast avsedda att användas vid utbildning.
Utbildningsnyckel	Nyckel som används vid utbildning. Observera att en utbildningsnyckel inte ger något signalskydd.
Utrustningsbehov	Myndighets/enhets behov av kryptonycklar inklusive utrustningsreserv under grundberedskap och under höjd beredskap.
Utrustningsklass	Anger en viss utrustnings RÖS-egenskaper. Klasserna indelas i klass U1, U2 och U3.
Utsändningsperiod (USP)	Periodicitet för utsändning av kryptonycklar.
Verifiering	Fastställande av riktighet.
Vilseledande signalering	Signalering i avsikt att försvåra signalunderrättelsetjänst och störsändning.
Visargrupp	Grupp av bokstäver som anger meddelandenyckel vid maskinchiffer eller vilken nyckelblankett som använts vid engångschiffer.
VPN-krypto	Virtuellt privat nätverk (Virtual Private Network). Kryptografiskt system som möjliggör höghastighetskommunikation mellan olika hemliga nätverkssegment över ett öppet icke pålitligt kommunikationsnätverk.
Yttre nyckel	Startvärde för kryptering som oftast varieras från meddelande till meddelande. Yttre nyckel kallas ibland även meddelandenyckel.

Äkthetskontroll	Medel och metod för att kontrollera ett meddelandes äkthet (autentisitet).
Övrig personal	Signalskyddslärare, användare, underhållspersonal samt förrådspersonal.

Register

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

Y

Å

Ä

Ö

FÖRSVARSMAKTEN
HÖGKVARTERET

107 85 Stockholm Tel 08 788 75 00 Fax 08-788 77 78

M7746-734002 H TST Grunder