FÖRSVARSMAKTEN
HÖGKVARTERET

FÖRSVARETS FÖRFATTNINGSSAMLING

FMLOG/TF-redaktionen
107 86 STOCKHOLM

ISSN 0347-7576

FFS 2005:2
Utkom från
trycket
2005-05-25

Försvarsmaktens föreskrifter om signalskyddstjänsten inom totalförsvaret;

beslutade den 16 maj 2005.

Försvarsmakten föreskriver med stöd av 39 § förordningen (2000:555) med instruktion för Försvarsmakten följande.

Inledande bestämmelser

1 § Föreskrifterna i denna författning gäller för statliga myndigheter.

2 § 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.

Definitioner

3 § I dessa föreskrifter avses med

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. s*ignalskyddsincident:* när en kryptonyckel har eller kan antas ha röjts (nyckelinicident) 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. s*ignalskyddspersonal*: 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.

Signalskyddsgrader

4 § 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/CONFIDENTIAL, 2. internationellt är klassad CONFIDENTIAL, eller 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.

Användning

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

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

Ledning och samordning

7 § 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.

8 § 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.

9 § 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.

Utbildning och behörighet

10 § 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.

11 § 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.

Kontroll av signalskyddstjänsten

12 § Varje myndighet skall genomföra kontroll av den egna signalskyddstjänsten. En kontroll skall avse instruktionen och säkerhetsskyddet för signal-

skyddstjänsten. 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.

Signalkontroll

13 § 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.

Kryptonycklar

14 § 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.

Produktion

15 § 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.

16 § 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.

Förpackning och distribution

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

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

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.

19 § 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.

Delgivning

20 § 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.

Hantering och förvaring

21 § 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.

22 § 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.

Redovisning och inventering

23 § 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.

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.

Rutinmässig förstöring

24 § 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.

Nyckelincident

25 § 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.

Signalskyddsmateriel

Utveckling och upphandling

26 § 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.

27 § 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.

Utförsel

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

Försegling

29 § 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.

Förpackning och distribution

30 § 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.

Redovisning och inventering

31 § 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.

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.

Placering och förvaring

32 § 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 Standardiserings-kommissionens normer (SIS), Svensk Standard (SS) 3492.

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

Överlåtelse av materiel

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

Materielincident

34 § 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.

Utlåning av materiel

35 § 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.

Avveckling och förstöring

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

Aktiva kort

37 § Aktiva kort indelas i

TAK, Totalförsvarets Aktiva Kort, avsett

- för identifiering av användare,
- för signering av information, eller
- som bärare av kryptonycklar,

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.

38 § 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.

39 § 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.

40 § 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.

Utgivning och personalisering

41 § 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.

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.

Förpackning, distribution och försändning

42 § 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.

43 § 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.

Utlämning

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

Hantering och förvaring

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

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.

Förlust

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

Undantag

47 § Försvarsmakten får medge undantag från föreskrifterna i denna författning.

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

Denna författning träder i kraft den 1 juni 2005.

Genom författningen upphävs Försvarsmaktens föreskrifter (FFS 1999:11) om signalskyddstjänsten inom totalförsvaret.

Håkan Syrén

Stefan Ryding-Berg