FÖRSVARSMAKTEN

FÖRSVARETS FÖRFATTNINGSSAMLING

FFS 2016:3

Utkom från trycket
2016-11-29

Försvarsmaktens föreskrifter om signalskyddstjänsten;

beslutade den 25 november 2016.

Försvarsmakten föreskriver med stöd av 33 § förordningen (2007:1266) med instruktion för Försvarsmakten följande.

1 kap. Allmänna bestämmelser

1 § Föreskrifterna i denna författning gäller för statliga myndigheter.

Definitioner

2 § I dessa föreskrifter avses med

1. *aktiva kort:* kort som är utgivna av Högkvarteret och som får innehålla signalskyddsnycklar samt har försetts med någon av följande benämningar:
   a) Totalförsvarets Aktiva Kort (TAK),
   b) Totalförsvarets Elektroniska ID-kort (TEID), eller
   c) Totalförsvarets Nyckelbärarkort (NBK),
2. *enhet:* en myndighets organisatoriska delar, såsom central ledning, regionala och lokala delar,
3. *hemlig uppgift:* uppgift som anges i 4 § 1 säkerhetsskyddsförordningen (1996:633),
4. *Högkvarteret:* Försvarsmaktens högkvarter,
5. *internationell signalskyddsöverenskommelse:* skriftlig överenskommelse som avser signalskydd mellan en svensk myndighet och en utländsk myndighet eller en mellanfolklig organisation,

6. *kryptografiska funktioner:* funktioner i ett system för

- att skydda information mot insyn och förvanskning, vid överföring och lagring med hjälp av kryptering,

- identifiering och autentisering,

- signering och verifiering av information, eller

- generering av signalskyddsnycklar,

7. *nyckelansvarig myndighet:* myndighet eller enhet som administrativt och operativt ansvarar för en viss nyckelserie,

8. *signalkontroll*: kontroll av signalskyddet i telekommunikations- och IT-system i syfte att klarlägga dels riskerna för obehörig åtkomst eller störande eller förvanskning av data, dels att systemen används enligt gällande författning samt de säkerhetsmässiga krav som Högkvarteret meddelar,

9. s*ignalskyddsincident:*

- när en signalskyddsnyckel har eller kan antas ha röjts (nyckelincident),

- när signalskyddsmateriel saknas eller kan antas ha manipulerats eller utsatts för åverkan (materielincident), eller

- när ett aktivt kort saknas, kan antas ha manipulerats eller att obehörig kan antas ha haft tillgång till kortet (incident med aktivt kort),

10. *signalskyddsmateriel:*

- kryptoapparat,

- komponent, utrustning eller programvara som innehåller, eller avses innehålla, kryptografisk funktion och som ingår, eller avses ingå, i ett signalskyddssystem samt

- annan signalskyddsspecifik materiel eller programvara,

11. *signalskyddsnycklar:* nycklar som direkt eller indirekt är avsedda att skydda hemliga uppgifter,

12. s*ignalskyddspersonal*: personal som har signalskyddsbefattning som signalskyddschef, biträdande signalskyddschef, systemoperatör, nyckeladministratör eller kortadministratör,

13. *signalskyddssystem:*

- system med kryptografiska funktioner som är godkänt av Högkvarteret för skydd av uppgifter enligt bilaga 1 till denna författning, eller

- system för skydd mot obehörig insyn i och påverkan av telekommunikations- och IT-system som är godkänt av Högkvarteret,

14. *signalskyddstjänst:* verksamhet som syftar till att förhindra obehörig insyn i och påverkan av telekommunikations- och IT-system med hjälp av kryptografiska metoder och övriga signalskyddsåtgärder,

15. *telekommunikationssystem*: system som innefattar tekniker för att överföra information mellan sändare och mottagare via ett trådlöst eller trådbundet medium.

Signalskyddsgrader

3 § I denna författning används begreppet signalskyddsgrader. Dessa indelas enligt följande: Top Secret (SG TS), Secret (SG S), Confidential (SG C), Restricted (SG R) samt Trafikskydd (SG TRF). Signalskyddsgradernas närmare betydelse anges i bilaga 1 till denna författning.

Användning av signalskyddssystem

4 § Varje myndighet som har anskaffat eller tilldelats ett signalskyddssystem ska följa denna författning samt de säkerhetsmässiga krav som Högkvarteret meddelar avseende systemet och dess ingående delar.

En myndighet får endast konfigurera och använda ett signalskyddssystem på det sätt som framgår av Högkvarterets godkännande av systemet.

Ledning och samordning av signalskyddstjänsten

5 § Varje myndighet eller enhet som har ett signalskyddssystem ska ha en signalskyddschef. 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, för en annan myndighet eller en eller flera av dess enheter efter överenskommelse mellan berörda myndigheter. En sådan överenskommelse ska

dokumenteras.

Vid varje myndighet eller enhet som har ett signalskyddssystem utan att ha en signalskyddschef ska det finnas en biträdande signalskyddschef.

6 § Varje myndighet eller enhet som har aktiva kort ska ha en eller flera kortadministratörer.

En myndighet eller enhet som endast nyttjar aktiva kort får i stället för en signalskyddschef ha en eller flera kortadministratörer. En kortadministratör ska ansvara för administration och redovisning av aktiva kort. Kortadministratörens rutiner ska dokumenteras.

7 § Vid en nyckelansvarig myndighet ska det finnas en eller flera personer som har genomgått utbildning till nyckelansvarig. Nyckelansvarig ska ha det administrativa ansvaret för en eller flera nyckelserier vid myndigheten.

Nyckelansvarig myndighets rutiner ska dokumenteras.

8 § En person får inneha flera signalskyddsbefattningar, roller eller ansvarsområden avseende signalskyddstjänsten vid en myndighet eller enhet som har ett signalskyddssystem.

9 § Varje myndighet och dess enheter som har ett signalskyddssystem ska i en handling (signalskyddsinstruktion) beskriva sin egen signalskyddsorganisation samt ange vilka åtgärder och uppgifter som krävs för att säkerställa signalskyddet, enligt bilaga 2 till denna författning. En sådan handling ska hållas uppdaterad.

Krav på utbildning och behörighet

10 § Endast den som med godkänt resultat har genomgått nödvändig utbildning i signalskydd får använda eller på annat sätt hantera signalskyddsmateriel, signalskyddsnycklar, aktiva kort eller inneha signalskyddsbefattning.

Varje myndighet ska se till att personalen ges nödvändig utbildning.

Den som har genomgått utbildning med godkänt resultat ska få ett behörighetsbevis.

11 § Ett behörighetsbevis enligt 10 § får endast utfärdas av Försvarsmakten eller av den som av Försvarsmakten har godkänts som utbildare i signalskydd.

Kontroll av signalskyddstjänsten

Internkontroll

12 § Varje myndighet eller enhet ska minst en gång per år, samt vid byte av signalskyddschef, genomföra kontroll av den egna signalskyddstjänsten. En kontroll ska avse myndighetens eller enhetens signalskyddsinstruktion och att gällande författning samt de säkerhetsmässiga kraven som Högkvarteret meddelar för signalskyddstjänsten följs. Det ska finnas en plan för hur denna kontroll ska genomföras.

Myndigheten eller enheten ska föra protokoll över varje kontroll. Protokollen ska bevaras i minst 10 år och hållas samlade.

Signalkontroll

13 § En myndighet eller enhet ska se till att signalkontroll genomförs i den omfattning som behövs för att konstatera om signalskyddet är tillräckligt.

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

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

2 kap. Signalskyddsnycklar

1 § Signalskyddsnycklar som är märkta med SG TS, SG S eller SG C får inte läsas in, förvaras, produceras eller användas i en utrustning som mellanlagrar signalskyddsnycklarna i klartext på permanent lagringsmedium.

Produktion

2 § Signalskyddsnycklar får endast produceras i utrustning samt med programvara och metoder som har godkänts av Högkvarteret.

Produktion av signalskyddsnycklar får endast ske på sådant sätt att obehöriga inte får insyn i verksamheten.

3 § Vid produktion av signalskyddsnycklar, som inte enbart existerar i elektronisk form, ska varje enskilt exemplar märkas med uppgift om vilket signalskyddssystem som nyckeln är avsedd för, nyckelserie, giltighetstid, lottningsnummer och signalskyddsgrad samt i förekommande fall kryptobeteckning.

Signalskyddsnycklar ska även förses med sekretessmarkering och exemplarnummer.

Produktion av signalskyddsnycklar ska dokumenteras. Av dokumentationen ska framgå vilket signalskyddssystem som nyckeln är avsedd för, nyckelserie, signalskyddsgrad, nyckelns giltighetstid, dess lottningsnummer och exemplarnummer.

Dokumentationen ska bevaras i minst 10 år efter det att respektive nyckel har upphört att gälla.

Avskrift eller kopiering

4 § En avskrift eller kopia av en signalskyddsnyckel får endast göras efter tillstånd av nyckelansvarig myndighet. Ett sådant tillstånd ska dokumenteras.

En avskrift eller kopia av en signalskyddsnyckel ska märkas med samma information som anges i 3 § första och andra styckena. En sådan avskrift eller kopia ska dokumenteras. Dokumentationen ska innehålla samma uppgifter som anges i 3 § tredje stycket.

Förpackning, distribution och mottagning

5 § Varje myndighet ska se till att nödvändiga skyddsåtgärder vidtas vid distribution av signalskyddsnycklar.

Signalskyddsnycklar som gäller och signalskyddsnycklar som har upphört att gälla får inte distribueras per post. Signalskyddsnycklar som inte har börjat gälla får distribueras per post.

Distribution av signalskyddsnycklar via telekommunikation får inte ske utan tillstånd av nyckelansvarig myndighet.

6 § Signalskyddsnycklar ska distribueras i ett förseglat emballage. Emballaget ska vara så beskaffat att det är omöjligt att ta del av innehållet utan att bryta emballaget. Förseglingen ska vara sådan att det går att se om någon har brutit emballaget.

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

7 § Distribution av signalskyddsnycklar ska dokumenteras.

8 § När signalskyddsnycklar distribueras ska ett mottagningsbevis och en följesedel bifogas i försändelsen. Av följesedeln ska framgå vilket signalskyddssystem som nyckeln är avsedd för, nyckelserie, nyckelns giltighetstid, dess lottningsnummer och exemplarnummer samt till vilken myndighet eller enhet respektive nyckel har distribuerats.

Följesedeln för signalskyddsnycklar som är märkta med SG TS ska registreras och bevaras i minst 25 år av avsändare och mottagare efter det att respektive nyckel har upphört att gälla.

Följesedeln för signalskyddsnycklar märkta med SG S, SG C, SG R eller SG TRF ska registreras och bevaras av avsändare och mottagare i minst 10 år efter det att respektive nyckel har upphört att gälla.

9 § Vid mottagning av en försändelse med signalskyddsnycklar ska innehållet i försändelsen skyndsamt kontrolleras mot bifogad följesedel. Mottagningsbeviset ska därefter snarast undertecknas och återsändas till avsändaren.

Överensstämmer inte innehållet i försändelsen mot bifogad följesedel ska avsändaren omedelbart underrättas.

Delgivning

10 § Signalskyddsnycklar får endast delges den som bedöms pålitlig ur säkerhetssynpunkt, har tillräckliga kunskaper om säkerhetsskydd, behöver nycklarna för sitt arbete i den verksamhet där de ska hanteras samt har fått nödvändig utbildning i signalskydd och hantering av signalskyddsnycklar.

Signalskyddspersonal som har tillgång till signalskyddsnycklar ska förtecknas. Övriga som delges signalskyddsnycklar ska kvittera mottagandet.

Förteckningar och kvittenser för signalskyddsnycklar märkta med SG TS ska bevaras i minst 25 år.

Förteckningar och kvittenser för signalskyddsnycklar märkta med SG S, SG C, SG R eller SG TRF ska bevaras i minst 10 år.

Hantering och förvaring

11 § Signalskyddsnycklar ska hanteras så att någon obehörig inte kan ta del av nyckeln.

12 § Signalskyddsnycklar som är märkta med SG TS, SG S eller SG C ska förvaras i ett utrymme som uppfyller lägst kraven för värdeskåp enligt Svensk Standard (SS) 3150 med lägre än 100 skyddsvärdespoäng, säkerhetsskåp enligt Svensk Standard (SS) 3492 eller Svensk Standard (SS-EN) 1143-1 grade 0-III eller stå under ständig uppsikt i syfte att uppnå erforderligt skydd.

Signalskyddsnycklar som är märkta med SG TS ska hållas åtskilda från signalskyddsnycklar som är märkta med en annan signalskyddsgrad.

Signalskyddsnycklar som är märkta med SG R eller SG TRF ska förvaras inlåsta eller förvaras i en lokal som endast den som är behörig att ta del av nycklarna har tillträde till eller stå under ständig uppsikt i syfte att uppnå erforderligt skydd.

13 § Varje myndighet eller enhet får först efter överenskommelse med nyckelansvarig myndighet fatta beslut som avviker från 12 § första stycket, under förutsättning att tillräcklig säkerhetsskyddsnivå kan upprätthållas. Ett sådant beslut ska dokumenteras.

Utförsel utanför svenskt territorium

14 § För att få föra ut eller på annat sätt göra signalskyddsnycklar tillgängliga utanför svenskt territorium krävs

1. att signalskyddsnycklarna är avsedda att användas för internationellt bruk, och
2. att nyckelansvarig myndighet, först efter överenskommelse med Högkvarteret, har beslutat att utförsel får ske samt hur nycklarna ska hanteras.

Signalskyddsnycklar som endast är avsedda att användas för nationellt bruk inom svenskt territorium får inte medföras utanför territoriet utan särskilt godkännande av Högkvarteret.

Inventering

15 § Inventering av signalskyddsnycklar ska göras vid ett långvarigt byte av signalskyddspersonal som ansvarar för signalskyddsnycklar.

Utöver vad som föreskrivs i första stycket ska odaterade signalskyddsnycklar inventeras varje år.

Signalskyddsnycklar som är märkta med SG TS ska inventeras av signalskyddschefen eller biträdande signalskyddschef samt ytterligare en signalskyddsutbildad person.

Signalskyddsnycklar med annan signalskyddsgrad ska inventeras av signalskyddschefen eller en av myndigheten utsedd signalskyddsutbildad person.

16 § Inventering av signalskyddsnycklar ska dokumenteras.

Dokumentationen avseende signalskyddsnycklar som är märkta SG TS ska bevaras i minst 25 år.

Dokumentationen avseende signalskyddsnycklar med en annan signalskyddsgrad ska bevaras i minst 10 år.

Rutinmässig förstöring och radering

17 § Varje signalskyddsnyckel ska snarast förstöras och, avseende nyckel som lagras elektroniskt, raderas när den har upphört att gälla eller när den inte längre behövs för tjänsten.

Förstöring av signalskyddsnycklar ska utföras av en signalskyddsutbildad person.

18 § Förstöring av signalskyddsnycklar ska dokumenteras.

Dokumentationen avseende signalskyddsnycklar som är märkta SG TS ska bevaras i minst 25 år.

Dokumentationen avseende signalskyddsnycklar med en annan signalskyddsgrad ska bevaras i minst 10 år.

19 § Signalskyddsnycklar ska förstöras på ett sådant sätt att det är omöjligt att återskapa och ta del av hela, eller delar av, signalskyddsnyckeln.

Åtgärder vid nyckelincident

20 § Den som har förlorat en signalskyddsnyckel eller misstänker eller på annat sätt har fått uppgift om att en signalskyddsnyckel kan vara röjd, ska omedelbart anmäla detta till nyckelansvarig myndighet och myndighetens eller enhetens signalskyddschef samt säkerhetsskyddschef.

Nyckelansvarig myndighet ska

1. avgöra om signalskyddsnyckeln kan ha röjts och meddela berörda enheter om vilka åtgärder som ska vidtas för att återställa signalskyddet, och

2. orientera den enhet i Högkvarteret som har till uppgift att leda och samordna signalskyddstjänsten inom totalförsvaret om vidtagna åtgärder och om anledningen till dessa.

3 kap. Signalskyddsmateriel

Utveckling och upphandling

1 § En myndighet som utvecklar eller tillverkar, eller låter utveckla eller tillverka materiel som avses bli signalskyddsmateriel ska se till att

1. det som grund för kravställning inför varje materielutveckling eller tillverkning görs en säkerhetsanalys och en säkerhetsplan som tar hänsyn till signalskyddets särskilda krav,

2. utveckling eller tillverkning av kryptoalgoritmer och övriga säkerhetsfunktioner i signalskyddsmateriel sker i IT-system som är godkända ur säkerhetssynpunkt (ackrediterade) först efter överenskommelse med Högkvarteret,

3. en hemlig kryptoalgoritm som är framtagen för ett visst system inte används i ett annat system utan skriftligt godkännande av Högkvarteret, och

4. sådan signalskyddsmateriel, signalskyddssystem eller del av signalskyddssystem, inte, utan godkännande av Högkvarteret, säljs eller överlämnas till någon annan än den myndighet som materielen är avsedd för.

Säkerhetsanalys och säkerhetsplan enligt första stycket 1 får fastställas först efter överenskommelse med Högkvarteret.

2 § En myndighet som upphandlar materiel som avses bli signalskyddsmateriel, eller programvara för sådan materiel, ska se till att leverantören förbinder sig att hantera materielen på ett sätt som säkerställer att den är säker att använda för avsett syfte.

Försegling och märkning

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

4 § Signalskyddsmateriel som innehåller kryptografiska funktioner, godkända för skydd av uppgifter enligt bilaga 1 till denna författning, ska vara märkt med

beteckningen SWE CCI (Swedish Controlled Cryptographic Item).

Signalskyddsmateriel som inte innehåller kryptografiska funktioner ska vara märkt med beteckningen SWE CI (Swedish Controlled Item).

Hantering

5 § Signalskyddsmateriel får endast hanteras av den som har tillräckliga kunskaper om säkerhetsskydd, behöver signalskyddsmaterielen för sitt arbete i den verksamhet där materielen ska hanteras samt med godkänt resultat har fått nödvändig utbildning i signalskydd.

Förpackning och försändning

6 § Vid försändning av signalskyddsmateriel ska emballaget vara så beskaffat att det är omöjligt att få information om materielen utan att bryta emballaget. Förseglingen ska vara sådan att det går att se om någon har brutit emballaget.

Vid mottagning av en försändelse med signalskyddsmateriel ska snarast

- emballagets försegling kontrolleras, samt
- innehållet i försändelsen kontrolleras mot bifogad följesedel eller kvitto.

Vid bruten försegling eller då innehållet i försändelsen inte överensstämmer mot bifogad följesedel eller kvitto ska avsändaren snarast underrättas.

Kvittering

7 § När signalskyddsmateriel lämnas ut ska signalskyddschefen eller den som lämnar ut materielen se till att signalskyddsmaterielen kvitteras av behörig användare eller signalskyddspersonal. Kvittensen ska bevaras under den tid som materielen är utlämnad.

Placering och förvaring

8 § En myndighet eller enhet ska vidta säkerhetsskyddsåtgärder i syfte att förhindra

manipulation och tillgrepp av signalskyddsmateriel. Åtgärderna ska dokumenteras.

Signalskyddsmateriel med inlästa signalskyddsnycklar ska hanteras och förvaras på samma sätt som föreskrivs om signalskyddsnycklar i 2 kap. 11–13 §§.

Utförsel av signalskyddsmateriel utanför svenskt territorium

9 § För att få föra ut signalskyddsmateriel utanför svenskt territorium krävs godkännande av Högkvarteret eller den enhet som Högkvarteret bestämmer.

Redovisning och inventering

10 § Varje myndighet eller enhet som har signalskyddsmateriel ska förteckna materielen i ett register. Av registret ska det framgå var materielen finns och dess individnummer. Registret ska ständigt hållas aktuellt.

11 § Signalskyddsmateriel som finns inom svenskt territorium ska inventeras varje år och signalskyddsmateriel som finns utomlands ska inventeras var sjätte månad. Inventering av signalskyddsmateriel ska även göras vid byte av befattningshavare som ansvarar för sådan materiel.

Signalskyddschefen ska se till att inventeringen utförs av en signalskyddsutbildad person.

Inventeringen ska dokumenteras och bevaras i minst 5 år.

Resultatet efter genomförd inventering ska kontrolleras mot enhetens register över signalskyddsmateriel. Brister som har framkommit i samband med en inventering ska utredas i syfte att klarlägga om det föreligger en materielincident eller inte. Utredningen ska dokumenteras.

Utlåning

12 § En myndighet får låna ut signalskyddsmateriel till någon som omfattas av föreskrifterna i denna författning. I övriga fall måste skriftligt avtal ha ingåtts mellan myndigheten och den som mottar materielen om att tillämpa innehållet i denna författning.

13 § Signalskyddsmateriel får lånas ut till en utländsk myndighet eller en mellanfolklig organisation endast om det finns en giltig internationell signalskyddsöverenskommelse.

Överlåtelse

14 § Signalskyddsmateriel får överlåtas endast till en annan statlig myndighet.

Avveckling och förstöring

15 § Vid avveckling av en enhets signalskyddsverksamhet eller när signalskyddsmateriel inte längre behövs ska materielen inventeras och återlämnas till den som tilldelat materielen. Inventeringen ska genomföras på det sätt som anges i 11 §.

16 § Signalskyddsmateriel får endast förstöras med en metod som är godkänd av Högkvarteret.

Åtgärder vid materielincident

17 § Den som har förlorat eller inte kan återfinna signalskyddsmateriel, eller misstänker manipulation av eller åverkan på signalskyddsmateriel eller dess försegling, ska omedelbart anmäla detta. Anmälan ska ske till myndighetens eller enhetens signalskyddschef, säkerhetsskyddschef och till den som tilldelat materielen samt till Högkvarteret.

Finns misstanke om att manipulation eller åverkan har skett på signalskyddsmateriel eller dess försegling ska materielen omedelbart tas ur drift.

4 kap. Aktiva kort

1 § 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.

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

Utgivning och personalisering

3 § En myndighet eller enhet som ska 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.

Aktiva kort ska förtecknas i ett register. Av registret ska framgå kortets serienummer, kortinnehavare samt i förekommande fall certifikat.

Förpackning och distribution

4 § Varje myndighet ska se till att nödvändiga skyddsåtgärder vidtas vid distributon av aktiva kort.

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

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

5 § När aktiva kort distribueras ska ett mottagningsbevis och en följesedel samt i förekommande fall kvitton bifogas. Av följesedeln ska framgå kortens serienummer och vem de är avsedda för. Följesedeln ska registreras vid mottagandet och bevaras i minst 10 år. Mottagningsbeviset ska snarast undertecknas och återsändas till avsändaren.

Vid mottagning av försändelse med aktiva kort ska innehållet i försändelsen snarast efter mottagandet kontrolleras mot bifogad följesedel. Överensstämmer inte innehållet i försändelsen med bifogad följesedel ska anmälan om incident med aktiva kort

omedelbart göras enligt vad som föreskrivs i 3 kap. 17 §.

Utlämning

6 § När aktiva kort ska lämnas ut ska användarens identitet kontrolleras och kortet ska därefter kvitteras av mottagaren.

Inläsning av signalskyddsnycklar

7 § Signalskyddsnycklar för samtliga signalskyddsgrader får läsas in i TAK och NBK enligt denna författning samt de säkerhetsmässiga kraven som Högkvarteret meddelar för signalskyddstjänsten. I ett TEID får endast signalskyddsnycklar för SG R och SG TRF läsas in.

Signalskyddsnycklar för olika signalskyddsgrader får inte samtidigt vara inlästa i samma aktiva kort med undantag för signalskyddsnycklar för SG S och SG C som får vara inlästa i samma aktiva kort, och signalskyddsnycklar för SG R och SG TRF som får vara inlästa i samma aktiva kort.

Ett aktivt kort med inlästa signalskyddsnycklar för SG TS får inte samtidigt ha inlästa signalskyddsnycklar med andra signalskyddsgrader.

För aktivt kort som har haft inlästa signalskyddsnycklar upp till och med SG R eller SG TRF ska byte av kortets kod göras innan signalskyddsnycklar för SG TS eller SG S och SG C läses in.

Hantering och förvaring

8 § Aktiva kort som innehåller signalskyddsnycklar ska hanteras och förvaras på samma sätt som föreskrivs om signalskyddsnycklar i 2 kap. 11–13 §§.

En myndighet eller enhet ska vidta säkerhetsskyddsåtgärder i syfte att förhindra manipulation och tillgrepp av aktiva kort utan inlästa signalskyddsnycklar. Åtgärderna ska dokumenteras.

Åtgärder vid incident med aktivt kort

9 § Den som har förlorat eller inte kan återfinna ett aktivt kort, misstänker eller på annat sätt har fått uppgift om att någon obehörig har haft tillgång till eller manipulerat ett aktivt kort, ska omedelbart anmäla detta. Anmälan ska ske till kortadministratör, myndighetens eller enhetens signalskyddschef och säkerhetsskyddschef samt till Högkvarteret.

5 kap. Internationella signalskyddsöverenskommelser

1 § En myndighet som förhandlar om att ingå en internationell signalskyddsöverenskommelse avseende svensk signalskyddsmateriel ska beakta föreskrifterna i denna författning. Endast om det föreligger särskilda skäl får myndigheten ingå en överenskommelse med lägre ställda krav på hantering och förvaring av signalskyddssystem än som framgår av denna författning.

Detta får ske först efter överenskommelse med Högkvarteret.

2 § Bestämmelserna i en internationell signalskyddsöverenskommelse avseende utländsk signalskyddsmateriel som ställer högre krav på hantering och förvaring av signalskyddssystem har företräde framför föreskrifterna i denna författning.

I övrigt har föreskrifterna i denna författning företräde.

6 kap. Undantag

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

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

Denna författning träder i kraft den 1 februari 2017.

Genom författningen upphävs Försvarsmaktens föreskrifter (FFS 2005:2) om signalskyddstjänsten inom totalförsvaret.

Micael Bydén

Carin Bratt

Bilaga 1

Signalskyddsgrader

Ett signalskyddssystem ska i samband med Högkvarterets godkännande placeras i någon av nedan angivna signalskyddsgrader med följande beteckningar och betydelser.

Beteckning	***Betydelse***
Signalskyddsgrad Top Secret (SG TS)	Signalskyddssystemet är godkänt för att skydda information som 1. är av synnerlig betydelse för rikets säkerhet (kvalificerat hemlig), 2. är placerad i informationssäkerhetsklassen HEMLIG/TOP SECRET, 3. har åsatts beteckningen TOP SECRET eller motsvarande av en utländsk myndighet eller mellanfolklig organisation, eller 4. om den röjs skulle förorsaka totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation synnerligt men.
Signalskyddsgrad Secret (SG S)	Signalskyddssystemet är godkänt för att skydda information som 1. är hemlig, 2. är placerad i informationssäkerhetsklassen HEMLIG/SECRET, 3. har åsatts beteckningen SECRET eller motsvarande av en utländsk myndighet eller mellanfolklig organisation, eller 4. om den röjs skulle förorsaka totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation betydande, men inte

Bilaga 1

	synnerligt, men.
Signalskyddsgrad Confidential (SG C)	Signalskyddssystemet är godkänt för att skydda information som 1. är hemlig, 2. är placerad i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL, 3. har åsatts beteckningen CONFIDENTIAL eller motsvarande av en utländsk myndighet eller mellanfolklig organisation, eller 4. om den röjs skulle förorsaka totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation inte obetydligt, men inte betydande eller synnerligt, men.
Signalskyddsgrad Restricted (SG R)	Signalskyddssystemet är godkänt för att skydda information som 1. är hemlig, 2. är placerad i informationssäkerhetsklassen HEMLIG/RESTRICTED, 3. har åsatts beteckningen RESTRICTED eller motsvarande av en utländsk myndighet eller mellanfolklig organisation, eller 4. om den röjs skulle förorsaka totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation endast ringa men.
Signalskyddsgrad Trafikskydd (SG TRF)	Signalskyddssystemet är godkänt för skydd av telekommunikation mot obehörig insyn i och påverkan av telekommunikations- och IT-system. Ett sådant signalskyddssystem (SG TRF) är dock inte godkänt för skydd av hemliga uppgifter.

Bilaga 2

Signalskyddsinstruktion

Enligt 1 kap. 9 § i denna författning ska signalskyddsinstruktionen innehålla uppgifter om

1. myndighetens eller enhetens signalskyddsorganisation,
2. åtgärder vid
- krishantering och höjd beredskap,
- signalskyddsincident,
3. enhetens signalskyddsutbildade personal, dess behörigheter och, i förekommande fall, placering i signalskyddsbefattning,
4. enhetens tilldelade signalskyddsnycklar samt var dessa förvaras,
5. rutiner för beställning, mottagning, extern och intern distribution, delgivning, kvittens, förvaring, inventering och förstöring av signalskyddsnycklar samt, i förekommande fall, lokal produktion av signalskyddsnycklar,
6. enhetens tilldelade signalskyddsmateriel samt var den är placerad och förvarad,
7. rutiner för beställning, mottagning, extern och intern försändning, utlämning, kvittens, förvaring, inventering, reparation och återlämning av signalskyddsmateriel,
8. enhetens register över aktiva kort, och
9. rutiner för beställning, mottagning, extern och intern försändning, utlämning, förvaring och återsändning av aktiva kort.