FÖRSVARSMAKTEN

FÖRSVARETS FÖRFATTNINGSSAMLING

FFS 2021:1

Utkom från trycket
2021-02-02

Försvarsmaktens föreskrifter om signalskyddstjänsten;

beslutade den 29 januari 2021.

Försvarsmakten föreskriver med stöd av 7 kap. 5 § första stycket 1 säkerhetsskyddsförordningen (2018:658) samt 33 § förordningen (2007:1266) med instruktion för Försvarsmakten följande.

1 kap. Inledande bestämmelser

1 § Denna författning gäller för en verksamhetsutövare som bedriver säkerhetskänslig verksamhet enligt 1 § säkerhetsskyddslagen (2018:585).

2 § I denna författning innefattar begreppet signalskyddstjänst kryptografiska funktioner som är avsedda för att skydda säkerhetskänslig verksamhet.

2 a § Förvaringskraven i denna författning gäller endast för de som inte ska tillämpa Riksarkivets, en kommuns eller en regions föreskrifter om gallring.

Definitioner

3 § I denna författning används följande begrepp och förkortningar med nedan angiven betydelse.

Begrepp	Betydelse
Aktiva kort	Kort som är godkända av Försvarsmaktens högkvarter och avsedda att användas i signalskyddstjänsten.
Certifikat	Digital information om utfärdare, innehavare samt signalskyddsnycklar som kan lagras på aktiva kort (hårda), CD, dator, kryptoapparat eller server (mjuka) och som är godkända av Försvarsmaktens högkvarter för användning i signalskyddstjänsten.
Elektroniskt kommunikationsnät	Ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs.
Enhet	En verksamhetsutövares organisatoriska del, såsom central ledning, regionala och lokala delar.
Internationell signalskyddsöverenskommelse	Skriftlig överenskommelse avseende signalskyddstjänst mellan Sverige och ett annat land eller mellanfolklig organisation.
Kryptoalgoritm	Matematiska funktioner i ett signalskyddssystem för skydd av information mot röjande och förvanskning, identifiering och autentisering,

	och generering av signalskyddsnycklar.
Totalförsvarets Nyckelbärarkort (NBK)	Ett aktivt kort som är godkänt av Försvarsmaktens högkvarter, får användas i signalskyddstjänsten samt får innehålla signalskyddsnycklar.
Nyckelansvarig verksamhetsutövare (NaV)	En verksamhetsutövare eller enhet som administrativt och operativt ansvarar för en viss nyckelserie.
Signalkontroll	Kontroll av signalskyddet i elektroniska kommunikationsnät och informationssystem i syfte att klarlägga dels riskerna för obehörig åtkomst eller störande eller förvanskning av data, dels att systemen används på avsett sätt.
Signalskyddsgrad	En indelning av ett signalskyddssystems kryptologiska styrka och vad signalskyddssystemet är godkänt för.
Signalskyddsincident	1. När en signalskyddsnyckel saknas eller har, eller kan antas ha, kommit till obehörigs kännedom (nyckelincident). 2. När signalskyddsmateriel saknas eller kan antas ha manipulerats eller utsatts för annan åverkan (materielincident). 3. När ett aktivt kort eller lagringsmedium för mjukt certifikat saknas, kan antas ha manipulerats eller att obehörig kan antas ha haft tillgång till kortet eller det mjuka certifikatet (incident med aktivt kort eller certifikat).

Signalskyddsmateriel	1. Kryptoapparat, komponent, utrustning eller programvara som innehåller, eller avses innehålla, kryptoalgoritmer och som ingår, eller avses ingå, i ett signalskyddssystem. 2. Annan signalskyddsspecifik materiel eller programvara.
Signalskyddsnycklar	Nycklar som är avsedda att användas i signalskyddstjänsten.
Signalskyddspersonal	Personal som har signalskyddsbefattning som signalskyddschef, biträdande signalskyddschef, systemoperatör, nyckeladministratör eller kortadministratör.
Signalskyddssystem	Av Försvarsmaktens högkvarter godkänt system som innehåller kryptoalgoritm för skydd av säkerhetskänslig verksamhet, inklusive säkerhetsskyddsklassificerade uppgifter, eller för trafikskydd.
Signalskyddstjänst	Verksamhet som syftar till att förhindra obehörig insyn i och påverkan av elektroniska kommunikationsnät och informationssystem, inklusive säkerhetsskyddsklassificerade uppgifter, med hjälp av signalskyddssystem och annan signalskyddsspecifik materiel eller programvara.
Totalförsvarets Aktiva Kort *(TAK)*	Ett aktivt kort för identifiering av användare och signering av information, som är godkänt av Försvarsmaktens högkvarter, får användas i

	signalskyddstjänsten samt får innehålla signalskyddsnycklar.
Totalförsvarets Elektroniska ID-kort *(TEID)*	Ett aktivt kort för identifiering av användare och signering av information, som är godkänt av Försvarsmaktens högkvarter, får användas i signalskyddstjänsten samt får innehålla vissa signalskyddsnycklar.
Trafikskydd	Skydd mot trafikanalys, falsk signalering och störsändning mot säkerhetskänslig verksamhet.

Signalskyddsgrader

4 § I denna författning används begreppet signalskyddsgrader. Signalskyddsgradernas närmare betydelse anges i bilaga 1 till denna författning.

Tilldelning av signalskyddssystem

5 § Den som enligt 16 § förordningen (2015:1053) om totalförsvar och höjd beredskap beslutar om vilka som ska tilldelas eller få tillgång till säkra kryptografiska funktioner får endast göra det genom tilldelning av nyttjanderätt.

Den som beslutar ska dessförinnan:

1. bedöma behovet av säkra kryptografiska funktioner och
2. säkerställa att mottagaren har de förutsättningar som krävs för att ta emot signalskyddssystemet.

6 § Den som enligt 17 § förordningen (2015:1053) om totalförsvar och höjd beredskap tilldelar en verksamhetsutövare signalskyddssystem som inte tidigare har tilldelats ett signalskyddssystem ska underrätta Försvarsmaktens högkvarter och berörd tillsynsmyndighet i samband med tilldelningen.

Användning av signalskyddssystem

7 § Ett signalskyddssystem är av betydelse för Sveriges säkerhet och får endast konfigureras och användas på det sätt som framgår av godkännande och de säkerhetsmässiga krav som Försvarsmaktens högkvarter meddelar avseende systemet och dess ingående delar.

Ledning och samordning av signalskyddstjänsten

8 § En verksamhetsutövare som har ett signalskyddssystem ska ha minst 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 hos en verksamhetsutövare, för en annan verksamhetsutövare eller en eller flera av dess enheter efter överenskommelse mellan berörda verksamhetsutövare. En sådan överenskommelse ska dokumenteras.

Hos en verksamhetsutövare eller enhet som har ett signalskyddssystem utan att ha en egen signalskyddschef ska det finnas en biträdande signalskyddschef.

9 § En verksamhetsutövare som har aktiva kort eller mjuka certifikat ska ha minst en kortadministratör.

En kortadministratör ska ansvara för administration och redovisning av aktiva kort och mjuka certifikat. Kortadministratörens rutiner ska dokumenteras.

Om det finns särskilda skäl får en kortadministratör vara kortadministratör för andra enheter hos en verksamhetsutövare, för en annan verksamhetsutövare eller en eller flera av dess enheter efter överenskommelse mellan berörda verksamhetsutövare. En sådan överenskommelse ska dokumenteras.

10 § Hos en nyckelansvarig verksamhetsutövare ska det finnas minst en person som har genomgått utbildning till nyckelansvarig. En nyckelansvarig ska ha det administrativa ansvaret för en eller flera nyckelserier vid verksamheten.

En nyckelansvarig verksamhetsutövares rutiner ska dokumenteras.

11 § En person får inneha flera signalskyddsbefattningar, roller eller ansvarsområden avseende signalskyddstjänsten hos en verksamhetsutövare eller enhet som har ett signalskyddssystem.

12 § En verksamhetsutövare och dess enheter som har ett signalskyddssystem ska dokumentera sin egen signalskyddsorganisation och vilka åtgärder och uppgifter som krävs för att säkerställa signalskyddet. Dokumentationen ska utformas enligt bilaga 2 till denna författning. Dokumentationen ska hållas uppdaterad.

I 2 kap. 1 § säkerhetsskyddslagen (2018:585) och 2 kap. 1 § säkerhetsskyddsförordningen (2018:658) finns föreskrifter om säkerhetsskyddsanalys och säkerhetsskyddsåtgärder. En verksamhetsutövare och dess enheter som har ett signalskyddssystem ska analysera signalskyddstjänstens särskilda krav på säkerhetsskydd och säkerställa att säkerhetsskyddet utformas så att dessa krav tillgodoses.

Krav på utbildning och behörighet

13 § Den som ska hantera signalskyddsmateriel, signalskyddsnycklar eller inneha signalskyddsbefattning ska ha behov av det för sitt arbete, vara pålitlig ur säkerhetssynpunkt, ha tillräckliga kunskaper om säkerhetsskydd samt vara placerad i lägst säkerhetsklass 3 eller motsvarande nivå som följer av en internationell signalskyddsöverenskommelse.

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

En verksamhetsutövare ska säkerställa att personalen ges nödvändig utbildning.

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

14 a § En verksamhetsutövare eller enhet ska förteckna all signalskyddsutbildad personal i ett register. Av registret ska det framgå personalens signalskyddsbehörigheter och, i förekommande fall, placering i signalskyddsbefattning. Registret ska hållas aktuellt.

14 b § Uppgifter om signalskyddsutbildad personal, dess behörigheter och, i förekommande fall, placering i signalskyddsbefattning ska förvaras så länge de behövs för verksamheten.

15 § Ett behörighetsbevis enligt 14 § får endast utfärdas av Försvarsmakten eller av den som av Försvarsmakten har godkänts som utbildare i signalskydd.

Tillsyn och kontroll av signalskyddstjänsten

16 § Den som ska utöva tillsyn över signalskyddstjänsten enligt 7 kap. 1 § säkerhetsskyddsförordningen (2018:658) ska årligen fastställa en plan för tillsyn som ska ligga till grund för tillsynsverksamheten. Planen ska uppdateras vid behov och på begäran lämnas till Försvarsmaktens högkvarter.

17 § Den som ska utöva tillsyn över signalskyddstjänsten ska genomföra tillsynen löpande och systematiskt samt skriftligen informera Försvarsmaktens högkvarter om det utförda arbetet.

18 § Den som utövar tillsyn över signalskyddstjänsten ska säkerställa att den som genomför tillsyn har relevant utbildning och är lämplig för uppgiften.

Kontroll

19 § En verksamhetsutövare eller enhet ska minst en gång per år, samt vid byte av signalskyddschef, genomföra kontroll av den egna signalskyddstjänsten. Kontrollen ska avse efterlevnaden av signalskyddsinstruktionen och denna

författning liksom de säkerhetsmässiga krav som Försvarsmaktens högkvarter meddelar för signalskyddstjänsten. Det ska finnas en plan för hur denna kontroll ska genomföras.

En verksamhetsutövare eller enhet ska föra protokoll över varje kontroll. Protokollen ska förvaras i minst 10 år och hållas samlade.

Signalkontroll

20 § En verksamhetsutövare eller enhet ska säkerställa att signalkontroll genomförs i den omfattning som behövs för att konstatera att signalskyddet är tillräckligt.

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

En verksamhetsutövare 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.

1 a § En verksamhetsutövare eller enhet som har signalskyddsnycklar ska förteckna dessa i ett register. Av registret ska det framgå vilka signalskyddsnycklar som hanteras av verksamhetsutövaren eller enheten samt var dessa förvaras. Registret ska hållas aktuellt.

1 b § Uppgifter om signalskyddsnycklar ska förvaras så länge de behövs för verksamheten.

Produktion

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

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.

Signalskyddsnycklar ska inte förses med anteckning om säkerhetsskyddsklass.

4 § 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 förvaras i minst 10 år efter det att respektive nyckel har upphört att gälla.

Avskrift eller kopiering

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

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

För avskrifter och kopior av signalskyddsnycklar gäller även vad som anges i 3 och 4 §§.

Förpackning, distribution och mottagning

6 § En verksamhetsutövare ska säkerställa 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 elektroniska kommunikationsnät får inte ske utan tillstånd av en nyckelansvarig verksamhetsutövare eller Försvarsmaktens högkvarter.

7 § 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 en verksamhetsutövare eller enhet har bestämt.

8 § En verksamhetsutövare ska besluta rutiner för hur signalskyddsnycklar ska distribueras. Rutinerna ska dokumenteras.

9 § 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 verksamhetsutövare eller enhet respektive nyckel har distribuerats.

10 § Följesedeln för signalskyddsnyckel som är märkt med SG TS, SG S, SG C, SG R eller SG TRF ska registreras.

11 § Avsändare och mottagare ska förvara följesedel för signalskyddsnyckel märkt med SG TS i minst 25 år efter att respektive nyckel har upphört att gälla.

Följesedeln för signalskyddsnyckel märkt med SG S, SG C, SG R eller SG TRF, ska förvaras i minst 10 år efter att respektive nyckel har upphört att gälla.

12 § 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

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

14 § Förteckningarna och kvittenserna för signalskyddsnycklar märkta med SG TS ska förvaras i minst 25 år.

Förteckningarna och kvittenserna för signalskyddsnycklar märkta med SG S, SG C, SG R eller SG TRF ska förvaras i minst 10 år.

Hantering och förvaring

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

16 § Signalskyddsnycklar som är märkta med SG TS, SG S eller SG C ska förvaras i ett utrymme som uppfyller lägst kraven för värdeskåp enligt norm SS 3150 med lägre än 100 skyddsvärdespoäng, säkerhetsskåp enligt norm SSF 3492 (SS 3492), standard SS-EN 1143-1 grade 0-III, kassaskåp enligt norm SS

3493 eller vara under kontroll 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 vara under kontroll i syfte att uppnå erforderligt skydd.

17 § En verksamhetsutövare eller enhet får först efter överenskommelse med en nyckelansvarig verksamhetsutövare fatta beslut som avviker från 16 § första stycket, under förutsättning att tillräcklig säkerhetsskyddsnivå kan upprätthållas. Ett sådant beslut ska dokumenteras.

Utförsel utanför svenskt territorium

18 § 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 en nyckelansvarig verksamhetsutövare, först efter överenskommelse med Försvarsmaktens högkvarter, har beslutat att utförsel får ske samt hur nycklarna ska hanteras.

Beslut enligt första stycket ska dokumenteras och dokumentationen ska förvaras i minst 10 år efter det att respektive nyckel har upphört att gälla.

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

19 § Av 4 § lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd följer att frågor om tillstånd och förbud enligt den lagen, eller föreskrifter som har meddelats med stöd av lagen, samt rådets förordning (EG) nr 428/2009 av den 5 maj 2009 om upprättande av en

gemenskapsordning för kontroll av export, överföring, förmedling och transitering av produkter med dubbla användningsområden, prövas av Inspektionen för strategiska produkter eller den myndighet som regeringen bestämmer.

Inventering

20 § 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 av en verksamhetsutövare utsedd signalskyddsutbildad person.

21 § Inventering av signalskyddsnycklar ska dokumenteras.

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

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

Rutinmässig förstöring

22 § Varje signalskyddsnyckel ska snarast förstöras när den har upphört att gälla eller när den inte längre behövs för tjänsten.

Förstöring av signalskyddsnycklar ska utföras av en signalskyddsutbildad person.

23 § Förstöring av signalskyddsnycklar ska dokumenteras.

Dokumentationen avseende signalskyddsnycklar som är märkta SG TS ska

förvaras i minst 25 år. Dokumentationen avseende signalskyddsnycklar med en annan signalskyddsgrad ska förvaras i minst 10 år.

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

Åtgärder vid nyckelincident

25 § Vid en inträffad nyckelincident ska anmälan omedelbart göras till en nyckelansvarig verksamhetsutövare och egen signalskydds- samt säkerhetsskyddsorganisation.

En nyckelansvarig verksamhetsutövare ska skyndsamt

1. avgöra om signalskyddsnyckeln ska tas ur drift och meddela berörda enheter om vilka åtgärder som ska vidtas för att återställa signalskyddet, och
2. orientera den enhet i Försvarsmaktens högkvarter som har till uppgift att leda och samordna signalskyddstjänsten inom totalförsvaret samt till den myndighet som med stöd av 7 kap. 1 § säkerhetsskyddsförordningen (2018:658) utövar tillsyn över verksamheten där incidenten inträffade om vidtagna åtgärder och om anledningen till dessa.

3 kap. Signalskyddsmateriel

Utveckling och upphandling

1 § Den som utvecklar eller tillverkar, eller låter utveckla eller tillverka, eller upphandlar, materiel som avses bli signalskyddsmateriel ska säkerställa att:

1. Utveckling och tillverkning av sådan materiel sker först efter överenskommelse med Försvarsmaktens högkvarter.
2. Den säkerhetsskyddsanalys enligt 2 kap. 1 § säkerhetsskyddslagen (2018:585) som ligger till grund för kravställning inför varje sådan materielutveckling eller tillverkning tar hänsyn till signalskyddets särskilda krav.
3. Utveckling och tillverkning av kryptoalgoritmer och övriga säkerhets-

funktioner i signalskyddsmateriel endast får ske i informationssystem som är godkända ur säkerhetssynpunkt. Godkännande kan ske först efter överenskommelse med Försvarsmaktens högkvarter.

4. En säkerhetsskyddsklassificerad kryptoalgoritm som är framtagen för ett visst system inte används i ett annat system utan skriftligt godkännande av Försvarsmaktens högkvarter.

5. Sådan materiel, samt signalskyddsmateriel, inte säljs eller överlämnas till någon annan än den upphandlande myndigheten, utan godkännande av Försvarsmaktens högkvarter.

6. Erforderlig säkerhet uppnås och påvisas.

Försegling och märkning

2 § 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.

3 § Signalskyddsmateriel som innehåller kryptoalgoritm, godkänd 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 kryptoalgoritm ska vara märkt med beteckningen SWE CI (Swedish Controlled Item).

Förpackning och försändning

4 § 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:

1. emballagets försegling kontrolleras, och

2. 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

5 § När signalskyddsmateriel lämnas ut ska signalskyddschefen eller den som lämnar ut materielen säkerställa att signalskyddsmaterielen kvitteras av signalskyddsutbildad användare eller signalskyddspersonal. Kvittensen ska förvaras under den tid som materielen är utlämnad.

Placering och förvaring

6 § En verksamhetsutövare 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. 15–17 §§.

Utförsel av signalskyddsmateriel utanför svenskt territorium

7 § För att få föra ut signalskyddsmateriel utanför svenskt territorium krävs godkännande av Försvarsmaktens högkvarter.

8 § Av 4 § lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd följer att frågor om tillstånd och förbud enligt den lagen, eller föreskrifter som har meddelats med stöd av lagen, samt rådets förordning (EG) nr 428/2009 av den 5 maj 2009 om upprättande av en gemenskapsordning för kontroll av export, överföring, förmedling och transitering av produkter med dubbla användningsområden, prövas av Inspektionen för strategiska produkter eller den myndighet som regeringen bestämmer.

Redovisning och inventering

9 § All signalskyddsmateriel ska vara registrerad i Försvarsmaktens centrala materielregister.

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

10 a § Uppgifter om signalskyddsmateriel ska förvaras så länge de behövs för verksamheten.

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 säkerställa att inventeringen utförs av en signalskyddsutbildad person.

Inventeringen ska dokumenteras och förvaras i minst 5 år.

Utlåning

12 § Den som tilldelats signalskyddsmateriel får låna ut materielen till någon som omfattas av denna författning.

Lån ska dokumenteras samt regleras i en skriftlig överenskommelse mellan verksamhetsutövarna. Den som tilldelat materielen ska informeras om lånet.

En enskild verksamhetsutövare som tilldelats signalskyddsmateriel får inte låna ut materielen.

12 a § Dokumentation över lån ska förvaras i minst 10 år efter utgången överenskommelse.

13 § Signalskyddsmateriel får lånas ut till en utländsk part endast om det finns en giltig internationell signalskyddsöverenskommelse.

14 § Av 4 § lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd följer att frågor om tillstånd och förbud enligt den lagen, eller föreskrifter som har meddelats med stöd av lagen, samt rådets förordning (EG) nr 428/2009 av den 5 maj 2009 om upprättande av en gemenskapsordning för kontroll av export, överföring, förmedling och transitering av produkter med dubbla användningsområden, prövas av Inspektionen för strategiska produkter eller den myndighet som regeringen bestämmer.

Avveckling och förstöring

15 § Vid avveckling av en verksamhetsutövares eller enhets signalskyddsverksamhet eller när signalskyddsmateriel inte längre behövs, eller inte längre är godkänd för användning, ska materielen inventeras och återlämnas till den som tilldelat eller lånat ut materielen.

Inventeringen ska genomföras på det sätt som anges i 11 §.

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

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 göras till en verksamhetsutövares eller enhets signalskydds- samt säkerhetsskyddsorganisation och till den som tilldelat materielen.

Försvarsmaktens högkvarter och den myndighet som med stöd av 7 kap. 1 § säkerhetsskyddsförordningen (2018:658) utövar tillsyn över verksamheten där incidenten inträffade ska skyndsamt orienteras.

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

4 kap. Aktiva kort och mjuka certifikat

1 § Aktiva kort och mjuka certifikat får endast användas på det sätt som framgår av godkännande från Försvarsmaktens högkvarter samt de säkerhetsmässiga krav som Försvarsmaktens högkvarter meddelar.

Certifikat ska inte förses med anteckning om säkerhetsskyddsklass.

2 § TAK och NBK får endast användas i kortterminaler eller kortläsare som har godkänts av Försvarsmaktens högkvarter. TAK och NBK får endast användas tillsammans med av Försvarsmaktens högkvarter godkända programvaror.

Utgivning och personalisering

3 § En verksamhetsutövare 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 Försvarsmaktens högkvarter.

Förpackning och distribution

4 § Aktiva kort och mjuka certifikat 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 mjuka certifikat och att det ska överlämnas obrutet till den som är kortadministratör eller till den som en verksamhetsutövare har bestämt.

5 § När aktiva kort och mjuka certifikat distribueras ska ett mottagningsbevis och en följesedel samt i förekommande fall kvitton bifogas. Av följesedeln ska serienummer på korten, de mjuka certifikatens lagringsmedium samt serienummer, och vem de är avsedda för, framgå. Följesedeln ska registreras vid mottagandet. Mottagningsbeviset ska snarast undertecknas och återsändas till avsändaren.

Följesedeln ska förvaras i minst 10 år.

6 § Vid mottagning av försändelse med aktiva kort och mjuka certifikat 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 och mjuka certifikat omedelbart göras enligt vad som föreskrivs i 3 kap. 17 §.

Redovisning

7 § En verksamhetsutövare eller enhet som har aktiva kort och mjuka certifikat ska förteckna dessa i ett register. Av registret ska framgå kortets eller det mjuka certifikatets serienummer, innehavare samt datum för ut- och återlämning.

8 § Uppgifter om aktiva kort och mjuka certifikat ska förvaras så länge de behövs för verksamheten.

Utlämning

9 § Till varje TAK, TEID och mjukt certifikat ska ett kvitto upprättas i två exemplar. När aktiva kort eller mjuka certifikat ska lämnas ut ska användarens identitet kontrolleras.

Ett kvittoexemplar ska efter kvittens av användaren återsändas till Försvarsmaktens högkvarter. Det andra kvittoexemplaret ska förvaras av använda-

ren. Kvittensliggare ska upprättas för ett aktivt kort som används av flera personer.

10 § Kvitton och kvittensliggare för aktiva kort som innehåller certifikat, samt kvitton och kvittensliggare för mjuka certifikat ska förvaras i minst 10 år efter att det aktiva kortet har återlämnats eller det mjuka certifikatet upphört att gälla.

Inläsning av signalskyddsnycklar

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

Signalskyddsnycklar för olika signalskyddssystem får inte samtidigt vara inlästa i samma aktiva kort.

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

12 § Aktiva kort som innehåller signalskyddsnycklar ska hanteras och förvaras på samma sätt som föreskrivs om signalskyddsnycklar i 2 kap. 15–17 §§.

13 § En verksamhetsutövare eller enhet ska vidta säkerhetsskyddsåtgärder i

syfte att förhindra manipulation och tillgrepp av aktiva kort utan inlästa signalskyddsnycklar. Åtgärderna ska dokumenteras.

Återlämning och förstöring

14 § När behovet av ett aktivt kort har upphört ska detta återlämnas till en verksamhetsutövares eller enhets kortadministratör. Kortadministratören ska säkerställa att det aktiva kortet återsänds till Försvarsmaktens högkvarter.

När ett giltigt mjukt certifikat inte längre behövs för tjänsten ska det förstöras. När ett mjukt certifikat har upphört att gälla ska anteckning göras på bäraren av det mjuka certifikatet om att dess märkning om sekretess inte längre är giltigt. Certifikatet får därefter kasseras.

15 § Aktiva kort och mjuka certifikat får endast förstöras med en metod som är godkänd av Försvarsmaktens högkvarter.

Åtgärder vid incident med aktivt kort eller mjukt certifikat

16 § Den som har förlorat eller inte kan återfinna ett aktivt kort eller mjukt certifikat, eller misstänker manipulation av aktivt kort eller mjukt certifikat, ska omedelbart anmäla detta. Anmälan ska göras till en verksamhetsutövares eller enhets signalskydds- samt säkerhetsskyddsorganisation och till den som tilldelat det aktiva kortet eller mjuka certifikatet, samt till Försvarsmaktens högkvarter och till den myndighet som med stöd av 7 kap. 1 § säkerhetsskyddsförordningen (2018:658) utövar tillsyn över verksamheten där incidenten inträffade.

Finns misstanke om att manipulation har skett på ett aktivt kort eller mjukt certifikat ska detta omedelbart tas ur drift.

5 kap. Internationella signalskyddsöverenskommelser

1 § Om det i en överenskommelse som avses i 10 kap. 1 eller 2 §§ regerings-

formen som rör ett visst internationellt samarbete förekommer bestämmelser om signalskyddstjänst som avviker från föreskrifterna i denna författning ska bestämmelserna i avtalet ha företräde.

Endast om det föreligger särskilda skäl får en sådan överenskommelse innehålla lägre ställda krav på hantering och förvaring av signalskyddssystem än som framgår av denna författning. Försvarsmaktens högkvarter ska informeras när en sådan överenskommelse har ingåtts.

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

I övrigt har 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.

———————

1. Denna författning träder i kraft den 1 mars 2021.
2. Genom författningen upphävs Försvarsmaktens föreskrifter (FFS 2019:9) om signalskyddstjänsten.

Micael Bydén

Kerstin Bynander

Bilaga 1

Signalskyddsgrader

Ett signalskyddssystem ska i samband med godkännande av Försvarsmaktens högkvarter 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 är placerad i säkerhetsskydds-klassen kvalificerat hemlig,
Signalskyddsgrad Secret (SG S)	Signalskyddssystemet är godkänt för att skydda information som är placerad i säkerhetsskydds-klassen hemlig,
Signalskyddsgrad Confi-dential (SG C)	Signalskyddssystemet är godkänt för att skydda information som är placerad i säkerhetsskydds-klassen konfidentiell,
Signalskyddsgrad Restricted (SG R)	Signalskyddssystemet är godkänt för att skydda information som är placerad i säkerhetsskydds-klassen begränsat hemlig,
Signalskyddsgrad Tra-fikskydd (SG TRF)	Signalskyddssystemet är godkänt för skydd mot trafikanalys, störsändning och falksignalering. Ett sådant signalskyddssystem (SG TRF) får användas för skydd av säkerhetskänslig verksamhet, dock inte för skydd av säkerhetsskyddsklassificerade uppgifter.

Bilaga 2

Signalskyddsinstruktion

En signalskyddsinstruktion ska minst innehålla uppgifter om:

1. En verksamhetsutövares eller enhets signalskyddsorganisation.

2. Åtgärder som ska vidtas vid krishantering, höjd beredskap och signalskyddsincident.

3. Rutiner för beställning, mottagning, extern och intern distribution, delgivning, kvittens, förvaring, inventering och förstöring av signalskyddsnycklar samt, i förekommande fall, lokal produktion av signalskyddsnycklar.

4. Rutiner för beställning, mottagning, extern och intern försändning, utlämning, kvittens, förvaring, inventering, reparation och återlämning av signalskyddsmateriel.

5. Rutiner för beställning, mottagning, extern och intern försändning, utlämning, förvaring och återsändning av aktiva kort och mjuka certifikat.