Sändlista se sidan 3

Ert tjänsteställe, handläggare
Signalskyddschefen

Ert datum

Er beteckning

Vårt tjänsteställe, handläggare
Peter Eidegren, 08-788 83 28,
peter.eidegren@mil.se

Vårt föregående datum

Vår föregående beteckning

Kommentarer till Försvarsmaktens föreskrifter (FFS 2021:1) om signalskyddstjänsten

(1 bilaga)

Bakgrund

Den 1 april 2019 trädde säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2018:685) i kraft. Av lagstiftningen följer att Försvarsmakten får meddela föreskrifter om kryptografiska funktioner som är avsedda för skydd av säkerhetskänslig verksamhet, utöver det bemyndigande för myndigheten som finns i 33 § förordningen (2007:1266) med instruktion för Försvarsmakten.

Överbefälhavaren beslutade Försvarsmaktens föreskrifter (FFS 2019:9) om signalskyddstjänsten 27 november 2019. Föreskriften trädde ikraft 1 januari 2020.

En tid efter det att FFS 2019:9 var beslutad påbörjades en omarbetning av föreskriften för att omhänderta ett antal förbiseenden samt upptäckta brister som var angelägna att rätta till.

Det resulterade i en ny förskrift, Försvarsmaktens föreskrifter (FFS 2021:1) om signalskyddstjänsten som Överbefälhavaren beslutade den 29 januari 2021. Föreskriften trädde i kraft 1 mars 2021 och då upphävdes också Försvarsmaktens föreskrifter (FFS 2019:9) om signalskyddstjänsten.

För att ge en bättre förståelse för föreskrifternas innebörd har säkerhetskontoret vid den militära underrättelse- och säkerhetstjänsten utarbetat kommentarer till dessa. Den primära målgruppen av kommentarerna är signalskyddspersonal, främst signalskyddschefer, hos verksamhetsutövare som bedriver

signalskyddstjänst. En förutsättning för att få full behållning av kommentarerna är att läsaren är utbildad inom signalskydd.

Läsanvisningar

Författningskommentarerna och den förklarande texten återfinns inramad i bilaga 1 medan originalföreskriftstexten är kursiverad.

Beslut

Beslut i detta ärende har fattats av tillförordnad avdelningschef kommendörkapten Fredrik Hjortsberg och som föredragande har varit sektionschef Peter Eidegren.

Hjortsberg, Fredrik

Tf Chef Avdelningen för krypto och IT-säkerhet

Handlingen är fastställd i Försvarsmaktens elektroniska dokument- och ärendehanteringssystem.

Sändlista

Riksdagsförvaltningen	
Sveriges riksbank	
Regeringskansliet	4 ex (avsett för UD Säk, Fö, RK Säk och FA IT INFRA SOSS)
AST	
LG	
I 19	2 ex (varav 1 ex för AJB)
K 3	
P 4	
P 7	
P 18	
A 9	
Lv 6	
Ing 2	
TrängR	
SWEDEC	
SkyddC	
MSS	
MS	
1.ubflj	
3.sjöstriflj	
4.sjöstriflj	
Amf 1	
MarinB	
SSS	
FS	
F 7	
F 17	
F 21	
Hkpflj	
LSS	
MR S	2 ex (avsedda för J2 och J6)
MR V	2 ex (avsedda för J2 och J6)
MR M	2 ex (avsedda för J2 och J6)
MR N	2 ex (avsedda för J2 och J6)
HvSS	
FMLOG	2 ex (varav 1 ex för Stab J2)
FMTS	
FömedC	
MHS K	
MHS H	
FM HRC	
LedR	3 ex (varav 1 ex vardera för TSS och TVK Ledsyst)
FMTIS	8 ex (avsett för J2, J5, J6, DriftE, SystE, SFE och SbE SbA)
FM UndSäkC	

SOG
Försvarets materielverk 2 ex (varav 1 ex avsett för Kjell Albiin)
Försvarets radioanstalt 2 ex (varav 1 ex avsett för Sollefteå)
Försvarsunderrättelsedomstolen
Kustbevakningen
Myndigheten för samhällsskydd och beredskap 2 ex (1 ex avsett för Karlstad)
Plikt- och prövningsverket
Statens inspektion för försvarsunderrättelseverksamhet
Totalförsvarets forskningsinstitut
Arbetsförmedlingen
Arbetsmiljöverket
Finansinspektionen
Riksgäldskontoret
Skatteverket
Statistiska centralbyrån (avsett för Helen Lindau i Örebro)
Tullverket (avsett för Stefan Bodis i Malmö)
Brottsförebyggande Rådet
Domstolsverket
Ekobrottsmyndigheten
Kriminalvården
Migrationsverket
Polismyndigheten avsett för Nationella IT-avdelningen (Per-Ove Povén) samt till Polisområdet i: Dalarna, Gotland, Gävleborg, Halland, Jämtland, Jönköping, Malmö, Norrbotten, ROE Toftanäs, Stockholm, Sydöstra Götaland Karlskrona, Södermanland, Uppsala, Värmland, Västerbotten, Västernorrland, Västmanland, Västra Götaland, Örebro och Östergötland
Rättsmedicinalverket
Säkerhetspolisen 6 ex (avsedda för Fredrik Ingemarsson och sektionerna)
Åklagarmyndigheten
Livsmedelsverket
Statens jordbruksverk
Statens veterinärmedicinska anstalt
Havs- och vattenmyndigheten
Strålsäkerhetsmyndigheten
Sveriges meteorologiska och hydrologiska institut (avsett för Norrköping)
Luftfartsverket (avsett för Norrköping)
Post och telestyrelsen
Sjöfartsverket
Statens energimyndighet
Svenska Kraftnät
Sveriges geologiska undersökning
Trafikverket
Transportstyrelsen 2 ex (avsedda för Sari Svensson och Trafikregistret)
eHälsomyndigheten
Folkhälsomyndigheten
Fortifikationsverket

Försäkringskassan
Lantmäteriet 2 ex (varav 1 ex vardera för Gävle och Geo-SE)
Läkemedelsverket
Länsstyrelsen i Blekinge, Dalarnas, Gotlands, Gävleborg, Halland, Jämtlands, Jönköpings, Kalmar, Kronobergs, Norrbottens, Skåne, Stockholms, Södermanlands, Uppsala, Värmlands, Västerbotten, Västernorrlands, Västmanlands, Västra Götalands (Göteborg + Vänersborg), Örebro och Östergötlands län
Socialstyrelsen
Statens fastighetsverk
Statens tjänstepensionsverk
Centrala Studiestödsnämnden
Försvarshögskolan
Folke Bernadotteakademin
Inspektionen för strategiska produkter
Sida
Kommunen i Stockholms stad, Västerås stad, Östersund och Linköping
Regioner/Landsting i Blekinge, Dalarna, Jämtland/Härjedalen, Kronoberg, Stockholms län och Västra Götalandsregionen
Forsmarks Kraftgrupp AB 742 03 Östhammar (avsett för Jan Karlsson)
OKG AB 572 83 Oskarshamn (avsett för Anders Nilsson)
Ringhals AB 432 85 Väröbacka (avsett för Jan Karlsson)
SOS Alarm Box 1309, 11183 Stockholm (avsett för Annika Nilshagen)
SSC-Esrange Space Center Box 802, 981 28 Kiruna (avsett för Richard Lidström)
Telia Sonera AB 405 35 Göteborg (avsett för Jonas Bergman)
Telia Sonera AB Box 336, 651 08 Karlstad (avsett för Helene Hammar)
Teracom AB Box 30150, 104 25 Stockholm (avsett för Johan Grufman)
Örebro läns flygplats AB 705 94 Örebro (avsett för Erik Johansson)
Jämtkraft AB Box 394, 831 25 Östersund
E.ON Carl Gustafs väg 1, 205 09 Malmö
Kemikalieinspektionen Box 2, 172 13 Sundbyberg

<u>Inom Högkvarteret</u>

HKV STAB (avsett för HKV signalskyddschef)
LEDS CIO
LEDS SFL
MUST LEDK 2 ex (1 ex avsett för MUST signalskyddschef)
MUST SÄKK
MUST SÄKK SÄKU
MUST SÄKK SÄKS
MUST SÄKK SÄKT
MUST IHK
PROD STAB
PROD RPE Ledsyst
PROD LEDUND

PROD LOG
INSS J2
INSS J6

Bilaga 1

Försvarsmaktens föreskrifter (FFS 2021:1) 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).*

Försvarsmaktens föreskrifter (FFS 2021:1) om signalskyddstjänsten, från och med nu benämnd i kommentarstexten som FFS signalskyddstjänst, gäller för alla som bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd, vilket sammantaget brukar benämnas säkerhetskänslig verksamhet. Detta inkluderar samtliga offentliga (statliga, regionala eller kommunala) och enskilda verksamhetsutövare, i enlighet med säkerhetsskyddslagen (2018:585), säkerhetsskyddsförordningen (2018:658) samt förordningen (2007:1266) med instruktion för Försvarsmakten.

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

Begreppet *”signalskyddstjänst”* är närmare definierat i 1 kap. 3 § och dess föreskriftsmandat återfinns i 33 § förordningen (2007:1266) med instruktion för Försvarsmakten. Meningen *”kryptografiska funktioner som är avsedda att skydda säkerhetskänslig verksamhet”* är tagen ordagrant ur 7 kap. 5 § säkerhetsskyddsförordningen och påvisar spårbarheten för Försvarsmaktens

detaljerade mandat inom sakområdet.

Då begreppet *”signalskyddstjänst”* är överordnat och bör användas som huvudbegrepp, uppnås på detta sätt en pedagogisk och förenklande fördel i och med att begreppet är välkänt sedan tidigare och nu har fått en utökad betydelse genom det nya föreskriftsmandatet i 7 kap. 5 § säkerhetsskyddsförordningen.

I enlighet med 3 kap. 5 § säkerhetsskyddsförordningen (2018:658) får endast kryptografiska funktioner som har godkänts av Försvarsmakten användas för att skydda säkerhetsskyddsklassificerade uppgifter om sådana uppgifter ska kommuniceras till ett informationssystem utanför verksamhetsutövarens kontroll. Detta innebär att de kryptografiska funktioner som avses och omnämns i FFS signalskyddstjänst endast ska förstås som Försvarsmaktsgodkända sådana och inte blandas ihop med civila, kommersiella eller liknande kryptografiska funktioner.

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

Tillkommande paragraf som omhändertar de liknande och upprepade skrivningar som återfanns i den upphävda FFS 2019:9. De upprepade skrivningarna är borttagna i denna nya FFS och har ersatts med denna paragraf.

Då Försvarsmakten inte har något mandat att föreskriva om gallring av handlingar reglerar denna FFS endast enskilda verksamhetsutövares, t.ex. företags, krav på förvaring. De förvaringskrav som återfinns i denna FFS överensstämmer med de föreskrifter om gallring, *Riksarkivets föreskrifter och allmänna råd (FA-FS 2021:3) om gallring av säkerhetshandlingar*, som Riksarkivet ger ut. Det är mycket viktigt ur ett signalskyddshänseende att dokumentation/handlingar som rör signalskyddstjänsten förvaras i enlighet med denna författning, detta då en spårbarhet måste kunna säkerställas för att främst omhänderta behovet av information för rättskipning.

Upplysningsvis kan i sammanhanget nämnas att arkivlagstiftningens huvudregel är att allmänna handlingar ska bevaras, men den medger ändå att information får gallras under förutsättning att den inte längre behövs för att tillgodose arkivlagens (SFS 1990:782) bevarandeändamål avseende rätten att ta

del av allmänna handlingar och behovet av information för rättskipning, förvaltning och forskning.

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.*

Certifikat som används inom signalskyddstjänsten kan delas in i två huvudkategorier:

1) hårda certifikat i form av försvarsmaktsgodkända aktiva (smarta) kort i fysisk form, t.ex. TAK, TEID och NBK vilka var och en beskrivs närmare under respektive begreppsförklaring i detta avsnitt ”*Definitioner*”, samt
2) mjuka certifikat i digital form lagrade på t.ex. CD-skivor, datorer, kryptoapparater eller servrar.

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.

Begreppet *"elektroniskt kommunikationsnät"* och dess definition är hämtat från 7 § lagen (2003:389) om elektronisk kommunikation och ska i denna föreskrift tolkas som fjärrkommunikationssystem eller telekommunikationssystem. Detta begrepp används även i flertalet andra FFS och FIB utgivna av Försvarsmakten.

Enhet	*En verksamhetsutövares organisatoriska del, såsom central ledning, regionala och lokala delar.*

Begreppet *"enhet*" är totalförsvarsneutralt definierat för att begreppet ska kunna omfatta verksamhet hos offentliga, privata samt enskilda verksamhetsutövare.

Internationell signalskydds-överenskommelse	*Skriftlig överenskommelse avseende signalskyddstjänst mellan Sverige och ett annat land eller mellanfolklig organisation.*

En skriftlig internationell signalskyddsöverenskommelse får endast förhandlas och ingås mellan en svensk myndighet och en utländsk myndighet eller internationell organisation, under förutsättning att den svenska myndigheten har ett giltigt regeringsbemyndigande att förhandla och ingå en sådan signalskyddsöverenskommelse.

Signalskyddsöverenskommelser benämns även exempelvis som signalskyddsavtal, COMSEC-avtal, Memorandum of Understanding (MoU), Memorandum of Agreement (MoA) eller Technical Agreement (TA)

I Försvarsmakten regleras sådana rutiner främst i Försvarsmaktens interna

bestämmelser (FIB 2017:9) internationella överenskommelser.

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.*

En omskrivning av den tidigare benämningen, Nyckelansvarig myndighet (NaM).

En Nyckelansvarig verksamhetsutövare (NaV) kan vara en verksamhetsutövare i form av en offentlig (statlig, regional eller kommunal) eller enskild verksamhetsutövare. Det kan finnas flera olika NaV och NaV-handläggare hos en verksamhetsutövare. En NaV-handläggares främsta uppgift är att driftsätta nyckelserier för att tillgodose verksamhetsutövarens (NaV) behov att skydda den egna verksamhetens information och behov av samverkan.

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.*

Signalskyddsnycklar ska ses som ett samlingsbegrepp för krypto-, system-, täck-, anrops-, lösen-, autentiserings-, frekvenshopps-, sessions-, privat- och packningsnycklar.

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.

Samtliga signalskyddsgrader räknas upp och beskrivs i detalj i bilaga 1.

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.

Den myndighet som utpekas enligt 16 § förordningen (2015:1053) om totalförsvar och höjd beredskap är Myndigheten för samhällsskydd och beredskap.

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.*

Den myndighet som utpekas enligt 17 § förordningen (2015:1053) om totalförsvar och höjd beredskap är Försvarets radioanstalt.

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.

Att signalskyddssystem är av betydelse för Sveriges säkerhet är en ny skrivning vilket bland annat innebär att användandet av signalskyddssystem i sig är en säkerhetskänslig verksamhet och därför omfattas även hantering och användandet av ett signalskyddssystem av det säkerhetsskydd som säkerhetsskyddslagstiftningen erbjuder.

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.

Signalskyddsverksamhetens omfattning kan vara vägledande om verksamhetsutövaren behöver fler än en signalskyddschef.

I de fall där en signalskyddschef agerar signalskyddschef för en annan verksamhetsutövare eller annan enhet inom egen organisation, se definition av enhet, är det av stor vikt att detta bereds, beslutas samt dokumenteras på ett korrekt sätt inom och mellan de berörda verksamhetsutövarna eller enheterna. Detta särskilt när det gäller en verksamhetsutövares verksamhetsutövning över en annan verksamhetsutövare eller dess enheter, vilket kan vara juridiskt komplicerat och behöver därför regleras skriftligen.

En sådan överenskommelse ska bevaras.

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.

Den dokumentation som avser rutiner ska dokumenteras i signalskyddsinstruktionen. Syftet är att dokumentationen ska klargöra och underlätta bedrivandet av en säker och kontinuerlig signalskyddsverksamhet för de olika certifikat som används inom signalskyddstjänsten.

Det är nu även möjligt för en kortadministratör att vara kortadministratör för andra verksamhetsutövare eller enheter, än sina egna.

I de fall där en kortadministratör agerar kortadministratör för en annan verksamhetsutövare eller annan enhet är det av stor vikt att detta bereds, beslutas samt dokumenteras på ett korrekt sätt inom och mellan de berörda verksamhetsutövarna eller enheterna. Detta särskilt när det gäller en verksamhetsutövares verksamhetsutövning över en annan verksamhetsutövare eller dess enheter, vilket kan vara juridiskt komplicerat och behöver därför regleras skriftligen.

En sådan överenskommelse ska bevaras.

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.

En nyckelansvarig verksamhetsutövare (NaV) ska företrädas av en nyckelansvarig handläggare som tillsammans med en uppdragsgivare ska ansvara för driftsättning av nya nyckelserier, reglera användning och tilldelning, besluta om åtgärder i samband med incidenter samt avveckla nyckelserier då dessa inte längre behövs i

verksamheten.

Dokumentationen kan med fördel nedtecknas i befintlig signalskyddsinstruktion, alternativt i ett särskilt framtaget dokument. Syftet är att dokumentationen ska klargöra och underlätta bedrivandet av en säker och kontinuerlig verksamhet för de nyckelserier som verksamhetsutövaren ansvarar för.

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

Denna paragraf har kommit till för att förtydliga att en person kan inneha flertalet signalskyddsbefattningar samtidigt.

En verksamhetsutövare rekommenderas av redundansskäl att ha mer än en utbildad person per signalskyddsbefattning, exempelvis fler än en utbildad signalskyddschef, biträdande signalskyddschef, nyckeladministratör, kortadministratör, signalskyddslärare och så vidare, då problem med bemanning och säkerställandet av signalskyddet oftast kan uppstå vid till exempel semester, sjukdom eller om personal slutar.

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.

Att ha en uppdaterad signalskyddsinstruktion är av största vikt för att kunna

upprätthålla en hög säkerhetsnivå för de signalskyddssystem som används. De uppgifter som framgår av bilaga 2 i enlighet med denna FFS utgör de grundläggande kraven som måste återfinnas i en signalskyddsinstruktion.

Övriga verksamhets- och säkerhetskrav som verksamheten ställer på signalskyddstjänsten kan även de dokumenteras i signalskyddsinstruktionen.

En signalskyddsinstruktion ska bevaras.

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.*

Det är av särskild vikt att personal som avses hantera signalskyddsmateriel och signalskyddsnycklar, innan de får tillgång till dessa, bedöms som lämplig och lojal enligt de kriterier som räknats upp. Detta då de sammantaget kan orsaka skada för Sveriges säkerhet, eftersom signalskyddsmateriel och signalskyddsnycklar ofta skyddar stora mängder säkerhetsskyddsklassificerade uppgifter inom flera olika ämnesområden (på en enda signalskyddsnyckel med stor spridning kan det aggregerat ha skickats stora mängder säkerhetsskyddsklassade handlingar mellan olika verksamhetsutövare).

Skälen för inplacering i säkerhetsklass 3, för sådan personal som räknas upp i paragrafen ovan, är följande:

- Signalskyddssystem, som bl.a. kan bestå av signalskyddsmateriel och signalskyddsnycklar, är enligt 1 kap. 7 § av betydelse för Sveriges säkerhet, vilket innebär att signalskyddssystem tydligt kan kopplas till bedrivande av säkerhetskänslig verksamhet och därför ska omfattas av säkerhetsskyddslagstiftningens säkerhetsskydd avseende personalsäkerhet och placering i säkerhetsklass av personal som hanterar signalskyddsmateriel och signalskyddsnycklar.

- Inneha signalskyddsbefattning syftar till ett deltagande i signalskyddsverksamhet och det är att likställa med att bedriva säkerhetskänslig verksamhet och kan om den bedrivs felaktigt orsaka skada för Sveriges säkerhet.

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.

Det är av största vikt att de som använder signalskyddssystem också vet hur de ska använda systemen och hur de ska hantera incidenter med systemet.

Normalt utbildar Totalförsvarets signalskyddsskola signalskyddschefer och signalskyddslärare. Verksamhetsutövaren med dess verksamheter har sedan normalt till uppgift att bland annat utbilda användare, systemoperatörer, förrådspersonal och nyckeladministratörer.

Behörighetsbevis skapar spårbarhet som bestyrker att utbildning skett med godkänt resultat. Denna paragraf ska samläsas med 13 §, vars krav utgör viktiga och säkerhetsmässiga förkunskapskrav vilka måste uppfyllas innan signalskyddsutbildning får ske.

14 a § *En verksamhetsutövare eller enhet ska förteckna all signalskyddsutbildad personal i ett register. Av registret ska det framgå personalens signal-skyddsbehörigheter 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.*

Tillkommande paragrafer som omhändertar det som tidigare stod uppräknat som krav på uppgifter som en signalskyddsinstruktion ska innehålla. Då en

signalskyddsinstruktion ska bevaras är det lämpligt att dessa register och personuppgifter inte återfinns i en signalskyddsinstruktion i enlighet med tidigare kommentar rörande denna författnings 1 kap. 2 a §.

Det är viktigt att personuppgifter endast förvaras så länge de behövs för verksamheten i syfte att värna enskildas rätt till skydd av personuppgifter genom att radera personuppgifterna när de inte längre behövs i enlighet med Dataskyddsförordningen (GDPR).

Denna paragraf medger att uppgifter får tas bort från registret i syfte att hålla det aktuellt.

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

Denna skrivning tydliggör att endast signalskyddslärare som utbildats av Försvarsmakten, samt andra signalskyddsbefattningar som får utbilda i signalskydd, får bedriva signalskyddsutbildning. En signalskyddslärare får utbilda personal även utanför egen organisation.

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.*

Regleringen av tillsynen för säkerhetsskyddet, vilket även omfattar tillsyn av signalskyddstjänsten som är en del av en informationssäkerhetsskyddsåtgärd, har fått ett vidgat begrepp i och med införandet av ny säkerhetsskyddslagstiftning, 7 kap 1-3 §§ säkerhetsskyddsförordningen (2018:658). Den regleringen har resulterat i dessa tre detaljerade paragrafer rörande tillsyn av signalskyddstjänsten. Paragraferna överensstämmer i huvudsak även med Säkerhetspolisens föreskrifter rörande tillsyn.

Den plan som beskrivs i 16 § bör även innehålla en förteckning över de

verksamheter som har signalskyddssystem inom tillsynsmyndighetens ansvarsområde. Ett sådant förfarande ligger i linje med utredningens förslag i betänkandet Kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82) avseende införandet av en skyldighet för tillsynsmyndigheter att systematiskt kartlägga verksamheter inom tillsynsmyndighetens ansvarsområde (7 kap. 3 a § förordning (2018:658) om ändring i säkerhetsskyddsförordningen). Av betänkandet framgår vidare att *”Närmare föreskrifter om hur arbetet med systematisk kartläggning och dokumentation av tillsynsobjekt ska gå till kan meddelas på föreskriftsnivå”* (2018:82 s. 410 f.).

Tillsynsmyndigheten bestämmer själv intervallerna för tillsynen och kan med fördel samordnas med övrig tillsyn av säkerhetsskyddet.

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

Normalt informerar tillsynsmyndigheten årligen 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.*

Med ”*relevant utbildning och är lämplig för uppgiften*” avses person som är inplacerad i lägst säkerhetsklass 3 samt med godkänt resultat åtminstone har genomfört av TSS anordnad utbildning till Signalskyddschef.

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.

Med ”*kontroll av den egna signalskyddstjänsten*” avses s.k. internkontroll av signalskyddstjänsten.
Syftet med internkontroll är att signalskyddschefen kritiskt ska granska den egna verksamheten i syfte att få en god uppfattning om signalskyddsverksamheten bedrivs enligt det som framgår av paragrafen. Om signalskyddschefen även är signalskyddschef över andra enheter eller verksamhetsutövare enligt 1 kap. 8 §. avser kontroll av den egna signalskyddstjänsten även den verksamheten.

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.

Med ”*fel eller brister som upptäckts vid kontrollen och som inte är av ringa betydelse anmälas till Försvarsmaktens högkvarter*” menas uppgifter som har placerats i säkerhetsskyddsklassen KONFIDENTIELL eller högre och vilka kan ha röjts på grund av fel eller brister i signalskyddet.

Det är verksamhetsutövaren själv som bestämmer vilken omfattning och med vilket intervall som signalkontroll ska genomföras, baserat på verksamhetsutövarens säkerhetsskyddsanalys och den säkerhetskänsliga verksamhetens art.

En verksamhetsutövare ska även skyndsamt anmäla till Säkerhetspolisen om de får kännedom om säkerhetshotande händelser eller verksamhet som uppdagats vid en signalkontroll.

I Försvarsmakten är det Försvarsmaktens Säkerhetsskyddschef som gör anmälan till Säkerhetspolisen enligt 8 kap. 2 §. Försvarsmaktens interna bestämmelser (FIB 2020:4) om säkerhetsskydd.

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.*

Med "*en utrustning som mellanlagrar signalskyddsnycklarna i klartext på permanent lagringsmedium*" menas till exempel en kopiator med hårddisk, en scanner, ett USB-minne etc. Det har hänt att användare har kopierat signalskyddsnycklar på kopiator med hårddisk ovetande om att signalskyddsnycklarna då sparats på kopiatorns hårddisk. En kopiator med hårddisk kan inte anses vara en säker lagringsplats samt att den är utanför användarens kontroll med tanke på exponering för servicepersonal, nätverksanslutningar och så vidare.

Signalskyddsnycklar som är märkta med SG R eller SG TRF får läsas in, förvaras, produceras eller användas i en försvarsmaktsgodkänd utrustning som mellanlagrar signalskyddsnycklarna i klartext på permanent lagringsmedium. En sådan försvarsmaktsgodkänd utrustning kan till exempel vara Lokal NyckelProduktion (LNP), där signalskyddsnycklarna på ett godkänt sätt mellanlagras i klartext på permanent lagringsmedium. Inte heller dessa signalskyddsnycklar får kopieras utan tillstånd av nyckelansvarig verksamhetsutövare.

1 a § *En verksamhetsutövare eller enhet som har signalskyddsnycklar ska förteckna dessa i ett register. Av registret ska det framgå vilka signalskydds-nycklar 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.*

Tillkommande paragrafer som omhändertar det som tidigare stod uppräknat som krav på uppgifter som en signalskyddsinstruktion ska innehålla. Då en signalskyddsinstruktion ska bevaras är det lämpligt att dessa register och uppgifter inte återfinns i en signalskyddsinstruktion i enlighet med tidigare kommentar rörande denna författnings 1 kap. 2 a §.

Denna paragraf medger att uppgifter får tas bort från registret i syfte att hålla det aktuellt.

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.

Produktion av signalskyddsnycklar sker centralt på Högkvarteret och/eller ute i verksamheten med produktionssystemet Lokal nyckelproduktion (LNP). Vissa signalskyddssystem kan även producera egna signalskyddsnycklar, tex PGBI och MGKI.

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.

En allmän märkning avseende sekretess görs på signalskyddsnycklar för att tillgodose lagkravet för bland annat sekretessmarkering enligt 5 kap. 5 § offentlighets- och sekretesslagen (SFS 2009:400).

Signalskyddsnycklar märks även med en s.k. signalskyddsgrad i enlighet med bilaga 1 i FFS signalskyddstjänst, vilken bl.a.:

- ger vägledning vid hantering och förvaring av signalskyddsnycklar och signalskyddsmateriel med inlästa signalskyddsnycklar,
- anger signalskyddssystemets maximala styrka, samt
- används vid märkning av signalskyddsnycklar för att ange vilken säkerhetsskyddsklass på informationen en viss nyckelserie är godkänd att skydda/kryptera.

Signalskyddsnycklar märks eller indelas inte i någon säkerhetsskyddsklass med stöd av 2 kap. 5 § säkerhetsskyddslagen (SFS 2018:585), då märkningen med signalskyddsgrad i stället tillgodoser korrekt hantering och förvaring ur perspektivet signalskyddstjänstens särskilda säkerhetsskydd. Försvarsmakten får enligt 3 kap. 7 § säkerhetsskyddsförordningen (SFS 2018:658) meddela föreskrifter inom sitt tillsynsområde om undantag från kravet på anteckning om säkerhetsskyddsklass, vilket uppnås med stöd av 7 kap. 1-2 §§ i samma förordning.

För signalskyddsnycklar och signalskyddstjänsten gäller ett särskilt regelverk i form av FFS signalskyddstjänst samt i förekommande fall säkerhetsmässiga krav för respektive signalskyddssystem, signalskyddsnycklar eller certifikat, vilket omfattar alla som hanterar signalskydd.

Se vidare bilaga 1 i denna skrivelse, för ytterligare vägledning hur signalskyddsgrader hänförs till relevanta säkerhetsskyddsklasser.

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.

Märkning och dokumentation av producerade signalskyddsnycklar är viktigt ur säkerhetssynpunkt och måste ske för att tilltron till systemet ska kunna hållas hög.

Vid gallring ska dock alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen.

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 §§.

Tillkommande författningstext vad gäller förvaringskrav för att tillgodose kravet på gallring i enlighet med tidigare kommentar rörande denna författnings 1 kap. 2 a §.

Avskrift eller kopiering av signalskyddsnycklar får endast undantagsvis göras och då mycket restriktivt. Risken med kopiering är att den som ska kopiera signalskyddsnyckeln använder fel sorts utrustning, vilket kan innebära att nyckeln exponeras otillbörligen och då kan anses vara röjd.

Vid gallring ska dock alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen.

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.

Signalskyddsnycklar som gäller samt signalskyddsnycklar som har slutat att gälla, får inte skickas med post. Anledningen är att nycklar som är eller har varit i drift med största sannolikhet har använts för att skydda säkerhetsskyddsklassificerade uppgifter eller säkerhetskänslig verksamhet och är då som mest skyddsvärd. Sårbarheten består i möjligheten för någon obehörig att komma åt nycklarna under transport, vilket kan få som konsekvens att obehörig har möjlighet att ta del av den information som skyddas med signalskyddsnycklarna. En avsändare måste säkerställa att signalskyddsnycklar inte heller börjar gälla under transporten. Avsändaren ska säkerställa att signalskyddsnycklarna har nått slutmottagaren senast två veckor innan de börjar gälla. I de fall signalskyddsnycklar inte nått slutmottagaren senast två veckor innan de börjar gälla ska slutmottagaren anmäla detta till avsändaren, utredning bör skyndsamt genomföras och om signalskyddsnycklarna fortfarande inte återfinns ska anmälan om nyckelincident omedelbart göras (se 2 kap 25§).

Signalskyddsnycklar som ännu inte har börjat gälla och där avsändaren vet att samtliga försändelser kommit fram till slutmottagaren får anses vara framgångsrikt levererade. En avsändare ska säkerställa en korrekt leverans genom användning av någon form av mottagningsbevis.

Distribution av signalskyddsnycklar via krypterad telekommunikation är med nuvarande teknik och tillgängliga lösningar en ur kryptologisk synpunkt dålig lösning då det skulle räcka för en motståndare att få tag på den första nyckeln som använts för att kryptera övriga nycklar för att sedan med hjälp av den få tag på alla andra nycklar.

För vissa signalskyddssystem och vissa signalskyddsnycklar kan det finnas särskilda hanteringsregler, exempelvis elektronisk distribution av

signalskyddsnycklar, om så är fallet framgår dessa i respektive signalskyddssystems säkerhetsmässiga krav.

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.

Emballage kan vara kuvert förseglat med säkerhetstejp eller en säkerhetspåse. Innerkuvertet syftar till att inte exponera nycklarna i onödan för exempelvis expeditionspersonal som tar emot försändelsen.

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

Dokumentationen av rutinerna görs i verksamhetsutövarens signalskyddsinstruktion enligt bilaga 2.

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.

Det är viktigt att mottagningsbeviset och följesedeln bipackas innerkuvertet där signalskyddsnycklarna finns. Detta för att det är signalskyddschefen eller annan utsedd person som tar emot nycklarna ska kunna kontrollera att alla nycklar finns med enligt följesedeln samt därefter snarast återsända mottagningsbeviset.

Försvarsmakten är numera en registratormyndighet vilket innebär att där en handling (exempelvis en följesedel) upprättas där ska handlingen också registreras. Då handlingar skickas och tas emot inom Försvarsmakten behöver mottagande enhet inte registrera handlingen eftersom den redan är registrerad av upprättande enhet. Är däremot handlingen att betrakta som inkommen från annan myndighet eller verksamhet ska den registreras där den inkom.

Vid gallring ska alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen.

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.

Det är för signalskyddstjänsten viktigt att innehållet kontrollräknas snarast efter det att försändelsen ankommit verksamhetsutövaren så att eventuella misstag kan rättas till i god tid innan nycklarna i försändelsen börjar att gälla.

Kontroll av innehållet behöver ske vid mottagandet, dock senast 3 veckor innan nycklarna börjar att gälla, så att en anmälan om fel kan rapporteras till avsändaren senast 2 veckor innan nycklarna börjar att gälla.

I de fall signalskyddsnycklar inte nått slutmottagaren senast två veckor innan de börjar gälla ska slutmottagaren anmäla detta till avsändaren, utredning bör skyndsamt genomföras och om signalskyddsnycklarna fortfarande inte återfinns ska anmälan om nyckelincident omedelbart göras (se 2 kap 25§).

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.

Kravet på bevarandet överensstämmer med de krav som finns för säkerhetsskyddsklassificerade handlingar enligt Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd samt Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

Vid gallring ska alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen.

Hantering och förvaring

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

I enlighet med 2 kap. 1 § säkerhetsskyddslagen (2018:585) ska den som bedriver säkerhetskänslig verksamhet utreda behovet av säkerhetsskydd (säkerhetsskyddsanalys). Säkerhetsskyddsanalysen ska dokumenteras.

Det innebär att verksamheten behöver göra en analys av hur signalskyddsnycklar hanteras och hur obehörig insyn kan förhindras. Lämpliga åtgärder kan exempelvis vara att dörrar till utrymmen där signalskyddsnycklar hanteras tillträdesbegränsas och förses med inpasseringskontroll och att insyn från fönster förhindras genom att gardiner dras för fönster vid hantering av nycklar. Nycklar bör inte heller hanteras på platser, exempelvis i en reception där obehörig personal normalt uppehåller sig och säkerhetsskåp som innehåller signalskyddsnycklar bör inte placeras i korridorer.

Detta gäller särskilt signalskyddsnycklar i pappersform som är mycket känsliga för exponering för obehöriga.

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.

De olika normerna och standarderna för säker fysisk förvaring av signalskyddsnycklar har uppdaterats i enlighet med nu gällande regelverk och överensstämmer i valda delar med de krav som finns för säkerhetsskyddsklassificerade handlingar enligt Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd samt Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

FFS signalskyddstjänst är tillämpningsbar för alla militära, civila och enskilda verksamhetsutövare som bedriver säkerhetskänslig verksamhet, medan Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd endast omfattar Fortifikationsverket, Försvarshögskolan samt de myndigheter som hör till Försvarsdepartementet. Med anledning av detta bör särskild hänsyn tas till främst de civila verksamhetsutövare som omfattas av signalskyddsföreskrifterna när det gäller de olika normerna och standarderna för säker fysisk förvaring av signalskyddsnycklar. Detta innebär i sin tur att Försvarsmaktens säkerhetsskyddsföreskrifters detaljerade och ofta militärt anpassade skyddsnivåer är svåra att tillämpa i signalskyddsföreskrifterna, vilka gäller för både militär och civil verksamhet där civila verksamhetsutövare förutom att ta hänsyn till signalskyddsföreskrifterna dessutom ska ta hänsyn till Säkerhetspolisens

föreskrifter (PMFS 2019:2) om säkerhetsskydd.

Den nu utgångna licensen till standarden SS 3492 har fortfarande ett tillräckligt säkerhetsskydd. Förvaras signalskyddsnycklar enligt denna standard uppfylls fortfarande kravet trots att licensen gått ut.

Signalskyddsnycklar märkta med SG TS ska hållas åtskilda, vilket innebär att nycklarna ska förvaras fysiskt separerade från andra signalskyddsnycklar i exempelvis en för ändamålet avsedd pärm, låda eller innerfack inne i det godkända förvaringsutrymmet.

Det nya begreppet ”*under kontroll*” avseende signalskyddsnycklar är mer pragmatiskt och ändamålsenligt i föreskriftstext än det tidigare begreppet ”*under ständig uppsikt*” samt överensstämmer i och med denna förändring med Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd.

Nyckelansvarig verksamhetsutövare (NaV) kan komma med ytterligare krav på förvaring i dennes driftsättningsskrivelse.

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.*

Detta överensstämmer med Försvarsmaktens föreskrifter (FFS 2019:2) om säkerhetsskydd och kan med fördel läsas som vägledning för hur en motsvarande skyddsnivå kan upprätthållas.

Ett sådant beslut ska bevaras.

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.

Nycklar som är avsedda för internationellt bruk ska vara märkta med tilläggsbeteckningen ”INT” i serienamnet (se Försvarsmaktspublikationen Säkerhetsmässiga krav för kryptonycklar 2010).

Nyckelansvarig verksamhetsutövare (NaV) är den verksamhet som driftsatt en nyckelserie för ett särskilt ändamål och det är av stor vikt att NaV har beslutat om utförsel först efter överenskommelse med avdelningen för krypto och IT-säkerhet (SÄKT) inom den militära underrättelse och säkerhetstjänsten (Must) vid Högkvarteret. Denna överenskommelse kan gälla över tid eller för en särskild verksamhet och behöver inte nödvändigtvis ske vid varje utförseltillfälle.

Vid Försvarsmakten finns ett särskilt godkännande i 29 § Försvarsmaktens interna bestämmelser (FIB 2008:3) om signalskyddstjänsten, att fartyg och luftfartyg som kortvarigt lämnar svenskt territorium för övningsverksamhet eller en nationell insats får föra ut de signalskyddsnycklar som oundgängligen behövs för att kunna genomföra övningen eller insatsen. Signalskyddsnycklarna ska om möjligt tas ur särskilda nyckelserier.

Tillkommande författningstext vad gäller förvaringskrav för att tillgodose kravet på gallring i enlighet med tidigare kommentar rörande denna författnings 1 kap. 2 a §.

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.

Detta innebär att verksamhetsutövare kan behöva söka utförseltillstånd hos Inspektionen för strategiska produkter (ISP) eller den myndighet som regeringen bestämmer. Vanligtvis är det ett globalt eller generellt utförseltillstånd som ansöks.

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.

Normalt behöver inte signalskyddsnycklar inventeras då de ska förstöras när de upphört att gälla eller inte längre behövs för tjänsten. Undantaget är odaterade nycklar, exempelvis beredskapsnycklar, som först på order tas i drift, eller andra lottningsnummernycklar som förvaras ute i verksamheten under lång tid innan användning. Med långvarigt byte menas exempelvis 6 månaders tjänstledighet eller utbildning, alltså längre än en normal semester på till exempel fyra till sex veckor.

Den personal som avses här är främst signalskyddspersonal med ansvar för en större mängd signalskyddsnycklar, men verksamhetsutövarens verksamhetsanalys och säkerhetsskyddsanalys bör ge svar på vad detta exakt innebär lokalt för varje verksamhetsutövare.

Det är viktigt att omständigheterna kring eventuella brister som framkommit

vid inventeringen utreds så att det kan vidtas nödvändiga åtgärder så att brister i förvaring och uppföljning inte upprepas. Förlust av signalskyddsnycklar är en signalskyddsincident och ska rapporteras och omhändertas enligt reglerna för signalskyddsincident i 25 §.

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.

Vid gallring av dokumentationen ska alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen.

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.

Det är av största vikt att de som använder signalskyddssystem också vet hur och när de ska förstöra signalskyddsnycklar på ett korrekt sätt.

Underrättelsevärdet för en signalskyddsnyckel är som högst när nyckeln har använts, eller används, vilket ställer höga krav på att alla exemplar av signalskyddsnycklarna förstörs när de har upphört att gälla eller inte längre behövs för tjänsten.

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.

Vid gallring av förstöringsliggare ska alltid beaktas att det arkivmaterial som

återstår ska kunna tillgodose behovet av information för rättskipningen.

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

Den förordade restprodukten/spånstorleken vid förstöring av signalskyddsnycklar (i pappersform) är 2 x 2 mm storlek eller mindre.

I övrigt så kan signalskyddsnycklar anses vara förstörda om restprodukten har en spånstorlek av 15 mm i längd och 1,2 mm i bredd eller mindre för att säkerställa att nyckeln inte ska kunna återskapas efter destruktion. Med denna typ av destruktion krävs det att signalskyddsnyckeln matas in så att destruktörens knivar skär parallellt med strecken i streckkoden.

Signalskyddsnycklar kan även förstöras genom eldning, viktigt att tänka på då är att sotflagor och restprodukter förbränns tills dess att det inte finns några restprodukter kvar än omrörd aska.

En signalskyddsnyckel kan inte anses vara helt förstörd förrän dess att även eventuella elektroniska kopior är raderade från kryptoapparater och olika lagringsmedia såsom aktiva kort, hårddiskar (för exempelvis LNP) samt att CD-skivor är förstörda.

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.

Tillkommande författningstext vad gäller att NaV även ska orientera berörd tillsynsmyndighet.

Anmälan om incidenter som berör signalskyddsnycklar ska omedelbart skickas till berörd/-a nyckelansvarig verksamhetsutövare (NaV) samt egen signalskydds- och säkerhetsorganisation.

Nyckelansvarig verksamhetsutövare (NaV) är ansvarig för att fatta beslut om vilka åtgärder som ska vidtas vid en incident som omfattar signalskyddsnycklar. En första åtgärd ska vara att snabbt fatta beslut och informera de signalskyddsorganisationer och användare som är tilldelade berörd nyckelserie om nyckeln ska tas ur drift eller inte, samt hur signalskyddet ska återställas så att ett säkert samband snarast kan återupprättas.

Då en signalskyddsincident även är en säkerhetsincident som påverkar informationssäkerheten vid en eller flera verksamhetsutövare rekommenderas att en utredning av omständigheterna kring incidenten genomförs. Syftet med utredningen är att komma fram till om berörda signalskyddsnycklar de facto är att betraktas som röjd, kan vara röjd eller inte är röjd. Utredningen bör genomföras av eller med stöd av säkerhetsorganisationen vid den enhet där incidenten inträffat och resultatet efter genomförd utredning ska skickas till berörd/-a NaV. NaV ansvarar därefter för att meddela resultatet till de verksamhetsutövare som är tilldelade de signalskyddsnycklar som omfattades av incidenten. Resultatet kan därefter utgöra grund för berörda verksamhetsutövarens beslut om eventuell menbedömning ska genomföras eller inte.

Orienteringen enligt punkten 2 ska NaV skriftligen skicka till Avdelningen för krypto och IT-säkerhet (SÄKT) vid Must Säkerhetskontor (vilket är den enhet i Försvarsmaktens högkvarter som har till uppgift att leda och samordna signalskyddstjänsten inom totalförsvaret). Samma orientering kan NaV även skriftligen skicka till den tillsynsmyndighet som har tillsynsansvaret över verksamheten där incidenten inträffade.

I orienteringen ska NaV sammanställa hela incidenten från inkommen incidentanmälan, eventuella kompletterande frågor, till slutligt beslut.

Orienteringen syftar till att SÄKT och tillsynsmyndigheten ska få en uppfattning över vilka incidenter som skett och varför samt utifrån det fatta beslut om åtgärder som kan stärka signalskyddstjänsten ytterligare. NaV uppmanas att sända in orienteringen enligt punkten 2 då det i nuläget inte sker alltför ofta.

En incident med en signalskyddsnyckel är att betrakta som en säkerhetsincident vilket innebär att även lokal säkerhetsorganisation behöver känna till det inträffade. Inom Försvarsmakten ska händelsen rapporteras som en säkerhetshändelse enligt Försvarsmaktens bestämmelser om säkerhetsskydd. För övriga verksamhetsutövare gäller respektive verksamhetsutövares säkerhetsbestämmelser.

En verksamhetsutövare, där en incident med signalskyddsnyckel har skett, har en skyldighet att skyndsamt och enligt Säkerhetspolisens bestämmande anmäla incidenten till Säkerhetspolisen då en incident med signalskyddsnyckel kan vara att betrakta som en säkerhetshotande händelse.

En verksamhetsutövare ska skyndsamt anmäla till Säkerhetspolisen om:
1. en säkerhetsskyddsklassificerad uppgift kan ha röjts,
2, det inträffat en it-incident i ett informationssystem som verksamhetsutövaren är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet, eller
3, verksamhetsutövaren får kännedom eller misstanke om någon annan för denne allvarlig säkerhetshotande verksamhet.

I Försvarsmakten är det Försvarsmaktens Säkerhetsskyddschef som gör anmälan till Säkerhetspolisen enligt 8 kap. 2 §. Försvarsmaktens interna bestämmelser (FIB 2020:4) om säkerhetsskydd.

Beakta alltid sekretessen vid kommunikation rörande signalskyddsincidenter.

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 säkerhetsfunktioner 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.

Denna paragraf riktar sig främst till Försvarsmaktens produktionsdelar och FMV som i sitt arbete utvecklar eller tillverkar, låter utveckla eller tillverka, eller upphandlar materiel som avses bli signalskyddsmateriel.

Det är viktigt att det finns en god dialog mellan FMV och Försvarsmakten för att bibehålla en hög säkerhetsnivå genom hela utvecklings- och tillverkningsprocessen.

Endast myndigheter har möjligheten att utveckla, tillverka, låta utveckla eller låta tillverka, eller upphandla signalskyddsmateriel på beställning.

Lydelsen ”*efter överenskommelse*” är ett starkare krav i författningstext än

lydelsen ”*samråd*”, vilken tidigare använts i signalskyddsföreskrifterna.

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.*

Försegling, plombering och lås är ett manipulationsskydd som är väsentligt för säkerheten kring signalskyddssystemen. För att uppnå hög säkerhet krävs att användaren regelbundet kontrollerar förseglingar, plomberingar och lås vid användandet av signalskyddssystemet.

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).

SWE CCI och SWE CI är internationellt erkända märkningar som tydliggör att det finns ett särskilt regelverk kring förvaring, hantering och användning av signalskyddssystem. SWE CCI-märkt signalskyddsmateriel innehåller i normalfallet en kryptomodul, till exempel kryptoapparat 491 i signalskyddssystem MGM (kryptofaxsystemet). SWE CI-märkt signalskyddsmateriel kallas även signalskyddsnära materiel och innehåller ingen kryptomodul men är väsentlig för att signalskyddssystemet ska fungera, till exempel själva faxen i signalskyddssystem MGM (kryptofaxsystemet).

Andra länder och internationella organisationer har normalt också märkningen ”CCI” eller ”CI”, ofta tillsammans med det egna landets eller organisationens förkortningsbeteckning, till exempel ”EU CCI”.

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.

Signalskyddsmateriel är att betrakta som skyddsvärd främst med tanke på dess tänkta användningsområde men även p.g.a. att utrustningen är dyr och finns i begränsad mängd. Med anledning av ovanstående ska signalskyddsmateriel försändas enligt myndighetens eller verksamhetsutövarens krav för skyddsvärd materiel.

Emballage kan vara kartong förseglat med säkerhetstejp eller säkerhetspåse. Det kan också vara transportbehållare med plombering eller där låsnycklar till transportbehållare samt eventuella låsnycklar till signalskyddsutrustning sänds separat med ”Postnord värde” eller motsvarande.

Det är för signalskyddstjänsten viktigt att innehållet kontrolleras skyndsamt så att eventuella misstag kan rättas till.

Försvarsmakten är numera en registratormyndighet vilket innebär att där en handling upprättas där ska handlingen också registreras. Då handlingar skickas och tas emot inom Försvarsmakten behöver mottagande enhet inte registrera handlingen eftersom den redan är registrerad av upprättande enhet. Är däremot handlingen att betrakta som inkommen från annan myndighet eller verksamhet ska den registreras där den inkom.

Handlingar som inte omfattas av sekretess behöver inte registreras om de hålls ordnade så att det utan svårighet kan fastställas om de har kommit in eller upprättats.

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.*

Då signalskyddsmateriel är att betrakta som skyddsvärd, och då främst med tanke på dess tänkta användningsområde, så ställer Försvarsmakten krav på dem som ska hantera den. För att uppnå en hög säkerhet krävs utbildning innan signalskyddssystemen får användas.

Signalskyddsmateriel är att betrakta som skyddsvärd främst med tanke på dess tänkta användningsområde men även p.g.a. att utrustningen är dyr, finns i begränsad mängd och därför behöver den kvitteras. Kvittering är också ett sätt att säkerställa personligt ansvar och detaljerad spårbarhet och uppföljning av signalskyddsmaterielen. En persons utbildningsstatus ska kontrolleras i samband med kvittering och nödvändig utbildning ska kunna styrkas av behörighetsbevis eller av uppgift i utbildningsregister.

Vid gallring ska dock alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen.

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 §§.

I enlighet med 2 kap. 1 § säkerhetsskyddslagen (2018:585) ska den som bedriver säkerhetskänslig verksamhet utreda behovet av säkerhetsskydd (säkerhetsskyddsanalys). Säkerhetsskyddsanalysen ska dokumenteras.

Det innebär att verksamhetsutövaren behöver göra en analys av vilka säkerhetsskyddsåtgärder som behöver vidtas för hur signalskyddsmateriel hanteras och hur obehörig insyn kan förhindras. Analysen bör belysa detta ur de båda perspektiven signalskyddsmateriel med inlästa eller inte inlästa signalskyddsnycklar.

Säkerhetsskyddsåtgärderna kan med fördel dokumenteras i signalskyddsinstruktionen och kan innehålla krav på att exempelvis utrymmen såsom kontorsrum och förråd där signalskyddsmateriel utan inlästa signalskyddsnycklar förvaras eller används ska hållas låsta om ingen behörig personal finns i utrymmet.

Utförsel av signalskyddsmateriel utanför svenskt territorium

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

Avdelningen för krypto och IT-säkerhet (SÄKT) inom den militära underrättelse och säkerhetstjänsten (Must) vid Försvarsmaktens Högkvarteret kan efter överenskommelse godkänna utförsel över tiden eller för en särskild verksamhet, s.k. stående utförseltillstånd.

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.*

Detta innebär att verksamhetsutövare även kan behöva söka utförseltillstånd hos Inspektionen för strategiska produkter (ISP) eller den myndighet som regeringen bestämmer. Vanligtvis är det ett globalt eller generellt utförseltillstånd som ansöks.

Redovisning och inventering

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

Med detta register menas Försvarsmaktens centrala materielregister vilket för närvarande är LIFT. Försvarsmakten eller FMV gör denna registrering för att uppnå strategisk kontroll och materieluppföljning.

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.*

Dokumentationen bör göras i ett av verksamhetsutövaren utpekat system, i verksamhetsutövarens lokala register, eller i ett separat dokument. Förteckningen ska, så långt det är möjligt, överensstämma med kvittenserna som gjordes vid utlämningen av signalskyddsmateriel.

En kontroll av att uppgifter i materielregistret överensstämmer med var befintlig materiel finns placerad ska även göras vid årlig inventering av signalskyddsmateriel.

Det är av stor vikt att registret ständigt hålls aktuellt för att garantera spårbarhet av signalskyddsmaterielen.

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.

Stöldrisken och underrättelsehotet bedöms vara större utomlands, vilket är anledningen till det strängare kravet vad gäller inventering av materiel utomlands.

Det är viktigt att omständigheterna kring eventuella brister som framkommit vid inventeringen utreds så att de som tilldelat materielen kan ersätta förlusten samt att verksamhetsutövaren kan vidta nödvändiga åtgärder så att brister i förvaring och uppföljning inte upprepas. Förlust eller manipulation av signalskyddsmateriel är en materielincident och ska rapporteras och omhändertas enligt reglerna för materielincident i 3 kap. 17 §.

Vid gallring ska dock alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen.

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.

Vid utlåning mellan verksamhetsutövare och annan avtalad verksamhet krävs kvittering av materielen enligt 3 kap. 5 §.

En ”*enskild verksamhetsutövare*” ska förstås på samma sätt som säkerhetsskyddslagstiftningen menar, d.v.s. näringsutövare som bedriver verksamhet som omfattas av säkerhetsskyddslagstiftningens bestämmelser inkluderande såväl företagsformer över vilka det allmänna har ett rättsligt inflytande som företagsformer där ett sådant inflytande inte finns. Typfallet är ett privat företag.

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.*

Signalskyddsmateriel får endast lånas ut till en annan nation, internationell organisation eller mellanfolklig organisation under förutsättning att ett gällande signalskyddsavtal enligt 5 kap. 1 § finns.
En signalskyddsöverenskommelse får endast upprättas av myndigheter som är bemyndigade av regeringen och signalskyddsöverenskommelsen blir giltig först efter att samtliga parter undertecknat den.

Innan signalskyddsmateriel förs utanför svenskt territorium ska Försvarsmakten godkänna utförseln enligt 3 Kap. 7 §.

Det kan också innebära att verksamhetsutövaren kan behöva söka utförseltillstånd hos Inspektionen för strategiska produkter (ISP) eller den myndighet som regeringen bestämmer. Vanligtvis är det ett globalt eller generellt utförseltillstånd som ansöks.

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.*

Detta innebär att verksamhetsutövare kan behöva söka utförseltillstånd hos Inspektionen för strategiska produkter (ISP) eller den myndighet som regeringen bestämmer. Vanligtvis är det ett globalt eller generellt utförseltillstånd som ansöks.

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 §.

När signalskyddsmateriel inte längre är godkänd för användning så kommer avvecklingen av systemet regleras i en teknisk order utgiven av Försvarets Materielverk (FMV).

Normalt återlämnas materiel inom Försvarsmakten samt de försvarsmaktsnära myndigheterna till Försvarsmaktsenheten FCIS och för övriga verksamhetsutövare till Försvarets Radioanstalt i Sollefteå.

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

Det är skillnad på kontrollerad förstöring av materiel, som exempelvis sker i samband med ett beslut om att avveckla ett signalskyddssystem och ett hastigt uppkommit behov, total eller begränsad förstöring, av att göra signalskyddsmaterielen obrukbar som kan behöva genomföras för att materielen inte ska falla i orätta händer i en kris eller krigsliknande situation i till exempel ett insatsområde.

I det första fallet ska materielen, efter reglering i en teknisk order utgiven av FMV, sändas tillbaka till centralt förråd som för Försvarsmakten samt de försvarsmaktsnära myndigheterna normalt är Försvarsmaktsenheten FCIS. För övriga verksamhetsutövare innebär det normalt Försvarets Radioanstalt i Sollefteå.

I det andra fallet gällande metoder för hastigt uppkommit behov av att göra signalskyddsmateriel obrukbar finns dessa i förekommande fall definierade i signalskyddssystemets säkerhetsmässiga krav. Följande åtgärder ska då vidtas:

1. Nödradering.
2. Signalskyddsmaterielen förstörs så att den blir obrukbar. Hur detta genomförs rent praktiskt avgörs av verksamhetens möjligheter att göra signalskyddsmaterielen obrukbar.

Notera att det krävs ytterligare åtgärder vid order om begränsad eller total förstöring förutom de två som beskrivs ovan, dessa ytterligare åtgärder återfinns i H TST Grunder 2007, bilaga 6.

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.

Tillkommande författningstext vad gäller att den som upptäcker en materielincident även ska orientera berörd tillsynsmyndighet.

Anmälan om materielincident ska göras till den som tilldelat materielen samt egen signalskydds- och säkerhetsorganisation.

Orienteringen enligt andra stycket ska skriftligen skickas till Avdelningen för krypto och IT-säkerhet (SÄKT) vid Must Säkerhetskontor (vilket är den enhet i Försvarsmaktens högkvarter som har till uppgift att leda och samordna signalskyddstjänsten inom totalförsvaret). Samma orientering ska även skriftligen skickas till den tillsynsmyndighet som har tillsynsansvaret över verksamheten där incidenten inträffade.

Orienteringen ska vara en sammanställning av hela incidenten. Orienteringen syftar till att SÄKT och tillsynsmyndigheten ska få en uppfattning över vilka incidenter som skett och varför samt utifrån det fatta beslut om åtgärder som kan stärka signalskyddstjänsten ytterligare. Verksamhetsutövare uppmanas att sända

in orienteringen enligt andra stycket då det i nuläget inte sker alltför ofta.

Tidigare krav på att signalskyddsmaterielen med bruten plombering eller annan upptäckt åverkan ska hanteras som hemlig är borttaget då materielen alltid ska betraktas som skyddsvärd och alltid ska hanteras så att manipulation och tillgrepp förhindras. Om signalskyddsmateriel tas ur drift p.g.a. en incident ska den överlämnas till signalskyddschefen eller annan lämplig signalskyddspersonal som ser till att materielen omhändertas på ett korrekt sätt intill dess att den kan skickas till utpekad kryptoverkstad. Utöver det ska en anmälan om materielincident upprättas.

En incident med en signalskyddsmateriel är att betrakta som en säkerhetsincident vilket innebär att även lokal säkerhetsorganisation behöver känna till det inträffade. Inom Försvarsmakten ska händelsen rapporteras som en säkerhetshändelse enligt Försvarsmaktens bestämmelser om säkerhetsskydd. För övriga verksamhetsutövare gäller respektive verksamhetsutövares säkerhetsbestämmelser.

Om det vid incidenten fanns inlästa signalskyddsnycklar i kryptoapparaten ska även en anmälan om nyckelincident upprättas enligt 2 kap. 25 §.

En verksamhetsutövare ska även skyndsamt anmäla till Säkerhetspolisen om de får kännedom om säkerhetshotande händelser eller verksamhet som uppdagats vid en materielincident.

En verksamhetsutövare ska skyndsamt anmäla till Säkerhetspolisen om:

1. en säkerhetsskyddsklassificerad uppgift kan ha röjts,
2. det inträffat en it-incident i ett informationssystem som verksamhetsutövaren är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet, eller
3. verksamhetsutövaren får kännedom eller misstanke om någon annan för denne allvarlig säkerhetshotande verksamhet.

I Försvarsmakten är det Försvarsmaktens Säkerhetsskyddschef som gör anmälan till Säkerhetspolisen enligt 8 kap. 2 §. Försvarsmaktens interna

bestämmelser (FIB 2020:4) om säkerhetsskydd.

Beakta alltid sekretessen vid kommunikation rörande signalskyddsincidenter.

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.

Certifikat ska inte förses med anteckning om säkerhetsskyddsklass, eftersom signalskyddsgraden, i enlighet med bilaga 1, FFS signalskyddstjänst, ersätter anteckning om säkerhetsskyddsklass.

Certifikatets signalskyddsgrad:

- ger vägledning vid hantering av certifikat,
- anger signalskyddssystemets maximala styrka, samt
- används vid märkning av certifikat för att ange vilken signalskyddsgrad ett visst certifikat är godkänt för.

Certifikat märks eller indelas inte i någon säkerhetsskyddsklass med stöd av 2 kap. 5 § säkerhetsskyddslagen (SFS 2018:585), då märkningen med signalskyddsgrad i stället tillgodoser korrekt hantering och förvaring ur perspektivet signalskyddstjänstens särskilda säkerhetsskydd. Försvarsmakten får enligt 3 kap. 7 § säkerhetsskyddsförordningen (SFS 2018:658) meddela föreskrifter inom sitt tillsynsområde om undantag från kravet på anteckning om säkerhetsskyddsklass, vilket uppnås med stöd av 7 kap. 1-2 §§ i samma förordning.

För certifikat gäller särskilda regelverk i form av FFS signalskyddstjänst och de förekommande säkerhetsmässiga krav för respektive signalskyddssystem, signalskyddsnycklar eller certifikat, vilket omfattar alla som hanterar signalskydd.

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.*

För TAK och NBK är godkända kortläsare normalt KT 2, KT USB, eller KT ADM. TEID får användas i kommersiella kortläsare.

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.

Emballage kan vara kuvert förseglat med säkerhetstejp eller säkerhetspåse. Innerkuvertet syftar till att inte exponera de aktiva korten eller mjuka certifikaten i onödan för exempelvis expeditionspersonal som tar emot försändelsen.

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.

Det är viktigt att mottagningsbeviset och följesedeln bipackas i det kuvert där de aktiva korten eller mjuka certifikaten finns. Detta för att det är kortadministratören eller någon annan utsedd person som tar emot de aktiva korten eller mjuka certifikaten som ska kontrollera att alla aktiva kort eller mjuka certifikat finns med enligt följesedeln samt därefter återsända mottagningsbeviset.

Det är för signalskyddstjänsten viktigt att innehållet kontrolleras skyndsamt så att eventuella misstag kan rättas till.

Försvarsmakten är numera en registratormyndighet vilket innebär att där en handling (exempelvis en följesedel) upprättas där ska handlingen också registreras. Handlingar som skickas och tas emot inom Försvarsmakten behöver mottagande enhet inte registrera då handlingen redan är registrerad av upprättande enhet. Är handlingen däremot att betrakta som inkommen från annan myndighet eller verksamhet ska den registreras där den inkom.
Vid gallring ska dock alltid beaktas att det arkivmaterial som återstår ska kunna tillgodose behovet av information för rättskipningen.

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.

Registret kan föras i ett av verksamhetsutövarens utpekat system (exempelvis TSA-rutinen i IS UNDSÄK eller CertOrder) eller i ett separat dokument.

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

Det är viktigt att personuppgifter endast förvaras så länge de behövs för verksamheten i syfte att värna enskildas rätt till skydd av personuppgifter genom att radera personuppgifterna när de inte längre behövs i enlighet med Dataskyddsförordningen (GDPR).

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

Det tidigare kravet på att det endast var kortadministratören som fick lämna ut aktiva kort är borttaget för att skapa handlingsutrymme vid verksamheter som hanterar aktiva kort. Totalförsvarets signalskyddsskola, TSS, har tagit fram ett utbildningsunderlag som kortadministratören kan använda vid utbildning av personal som endast ska lämna ut och ta emot aktiva kort.

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.*

Användaren ska upplysas om hur kvitton och dataposter ska förvaras och hanteras samt att handlingarna ska finnas tillgängliga vid behov.

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.

Tillkommande författningstext vad gäller att signalskyddsnycklar för olika signalskyddssystem inte samtidigt får vara inlästa i samma aktiva kort. Aktiva kort med inlästa signalskyddsnycklar övertar nycklarnas klassning när de är inlästa i det aktiva kortet enligt 2 kap. 15-17 §§. Byte av kod på aktiva kort som har haft inlästa signalskyddsnycklar upp till och med SG R eller SG TRF syftar till att minska intrångsrisken då det aktiva kortet har använts i signalskyddssystem med en lägre skyddsnivå.

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 §§.*

Se förutvarande kommentar avseende 4 kap. 11 §.

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

I enlighet med 2 kap. 1 § säkerhetsskyddslagen (2018:585) ska den som bedriver säkerhetskänslig verksamhet utreda behovet av säkerhetsskydd (säkerhetsskyddsanalys). Säkerhetsskyddsanalysen ska dokumenteras. Det innebär att verksamhetsutövaren behöver göra en analys på vilka säkerhetsskyddsåtgärder som behöver vidtas för hur manipulation och tillgrepp ska förhindras.

Säkerhetsskyddsåtgärderna kan sedan med fördel dokumenteras i signalskyddsinstruktionen och kan innehålla krav på att exempelvis kontorsrum, där aktiva kort utan inlästa nycklar används, ska hållas låsta om ingen behörig personal finns i utrymmet. Vidare kan exempelvis ett krav vara att ett aktivt kort, utan inlästa nycklar, ska hanteras som användarens bankkort.

Datapost för TAK och NBK ska hållas under ständig uppsikt eller förvaras inlåst i säkerhetsskåp. Datapost för TEID ska skyddas mot manipulation och tillgrepp till exempel genom ständig uppsikt, vara under kontroll eller förvaring i ett låst utrymme.

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.

Regleringen av mjuka certifikat är ny i dessa föreskrifter och målsättningen är att undvika en för hög detaljeringsgrad, då de specifika detaljerade kraven för dessa

i stället ska återfinnas i till exempel manualer, reglementen och skrivelser.

Ett mjukt certifikat ska aldrig sparas eller arkiveras efter att det slutat att gälla, det ska i stället raderas från den utrustning det har varit inläst i. Sekretessmarkeringen på det medium som certifikatet levererats på ska sedan upphävas enligt direktiv i skrivelse FM2020-922:1 ”Direktiv kring destruktion av CD som innehåller mjukt certifikat”, därefter kan mediet slängas, det behöver inte längre förstöras.

Rutinen för mjuka certifikat som har revokerats (har återkallats men fortfarande har giltighetstid kvar) har gjorts om för att efterlikna hanteringen av signalskyddsnycklar, d.v.s. media innehållande mjuka certifikat får nu förstöras av behörig personal. Förstöring och destruktion ska principiellt ske så nära slutanvändaren som möjligt, detta för att minimera risken för att CD-skivor förvaras och exponeras mer än nödvändigt. Exponering ska även tas hänsyn till i samband med postförsändning av media innehållande certifikat, då certifikaten innehåller information om bland annat organisationsenhet, personuppgifter, servernamn och giltighetstider.

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

Vad gäller mjuka certifikat på CD-skiva så kan det informationsbärande metallskiktet på CD-skivan slipas ner antingen för hand eller med en slipmaskin ämnad för att just slipa ner det informationsbärande informationsskiktet. Det viktiga är att restprodukten efter slipningen är damm.

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.

Tillkommande författningstext vad gäller att den som upptäckt en incident med aktivt kort eller mjukt certifikat även ska anmäla händelsen till berörd tillsynsmyndighet.

När det gäller incidenter som berör aktiva kort så är det innehållet på det aktiva kortet (exempelvis nycklar och certifikat) som styr hur en incidentanmälan ska göras men även tomma aktiva kort ska incidentanmälas. Anmälan om incident med aktivt kort eller mjukt certifikat ska anmälas till egen signalskydds- och säkerhetsorganisation samt den som tilldelat berört aktivt kort eller mjukt certifikat. Med den som tilldelat menas i detta fall den person, enhet eller verksamhet som hjälper en verksamhetsutövare (som inte själv har tillgång till beställningssystemen) med beställningar.

Anmälan till Försvarsmaktens högkvarter enligt första stycket avser den sektion inom Avdelningen för krypto och IT-säkerhet vid MUST säkerhetskontor som ansvarar för certifikat- och nyckelproduktion (HKV MUST SÄKK SÄKT NF). En revokering av ett aktivt kort, som innehåller certifikat, eller mjukt certifikat, är för denna paragraf att betrakta som en anmälan till Försvarsmaktens högkvarter, och görs normalt av ansvarig kortadministratör.

Anmälan ska även skriftligen skickas till den tillsynsmyndighet som har tillsynsansvaret över verksamheten där incidenten inträffade. Anmälan till tillsynsmyndigheten ska vara en sammanställning av hela incidenten och kan ha samma orienterande karaktär som en anmälan till tillsynsmyndighet vad gäller en nyckel- eller materielincident. Anmälan syftar till att tillsynsmyndigheten ska få en uppfattning över vilka incidenter som skett och varför. Tillsynsmyndigheten kan utifrån informationen i anmälan fatta beslut om åtgärder som ytterligare kan stärka säkerheten som omgärdar signalskyddstjänsten vid verksamhetsutövare som tillsynsmyndigheten bedriver tillsyn över.

En incident med aktiva kort eller mjukt certifikat är att betrakta som en

säkerhetsincident vilket innebär att även lokal säkerhetsorganisation behöver känna till det inträffade. Inom Försvarsmakten ska händelsen rapporteras som en säkerhetshändelse enligt Försvarsmaktens bestämmelser om säkerhetsskydd. För övriga verksamhetsutövare gäller respektive verksamhetsutövares säkerhetsbestämmelser.

En verksamhetsutövare ska även skyndsamt anmäla till Säkerhetspolisen om de får kännedom om säkerhetshotande händelser eller verksamhet som uppdagats vid en incident med aktiva kort eller mjukt certifikat.

En verksamhetsutövare ska skyndsamt anmäla till Säkerhetspolisen om:

1. en säkerhetsskyddsklassificerad uppgift kan ha röjts,
2. det inträffat en it-incident i ett informationssystem som verksamhetsutövaren är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet, eller
3. verksamhetsutövaren får kännedom eller misstanke om någon annan för denne allvarlig säkerhetshotande verksamhet.

I Försvarsmakten är det Försvarsmaktens Säkerhetsskyddschef som gör anmälan till Säkerhetspolisen enligt 8 kap. 2 §. Försvarsmaktens interna bestämmelser (FIB 2020:4) om säkerhetsskydd.

Beakta alltid sekretessen vid kommunikation rörande signalskyddsincidenter.

5 kap. Internationella signalskyddsöverenskommelser

1 § *Om det i en överenskommelse som avses i 10 kap. 1 eller 2 §§ regeringsformen 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.

När utländsk personal ska använda svenska signalskyddssystem ska de normalt använda och hantera systemet på samma sätt som svensk personal. Samma krav på behörighet, i form av bland annat motsvarande personalsäkerhetskrav, behov av att använda svenska signalskyddssystem för sin tjänst samt signalskyddsutbildning, ska gälla.

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.

Vid hantering av utländska signalskyddssystem gäller som grund de svenska reglerna för signalskyddstjänsten. Det kan dock tillkomma ytterligare och hårdare krav såsom att utländsk materiel inte får postförsändas utan endast får transporteras av utbildad personal. Utländska signalskyddssystem som tilldelats Sverige som slutanvändarland får i normalfallet dessutom aldrig lånas ut eller säljas till något annat land och inte heller exponeras för utländska medborgare.

6 kap. Undantag

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

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

Överbefälhavaren har inte beslutat att någon annan än Överbefälhavaren får fatta 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.

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 säkerhetsskyddsklassen kvalificerat hemlig,*
Signalskyddsgrad Secret (SG S)	*Signalskyddssystemet är godkänt för att skydda information som är placerad i säkerhetsskyddsklassen hemlig,*
Signalskyddsgrad Confidential (SG C)	*Signalskyddssystemet är godkänt för att skydda information som är placerad i säkerhetsskyddsklassen konfidentiell,*
Signalskyddsgrad Restricted (SG R)	*Signalskyddssystemet är godkänt för att skydda information som är placerad i säkerhetsskyddsklassen begränsat hemlig,*
Signalskyddsgrad Trafikskydd (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.*

Varje signalskyddssystem 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 signalskyddsnycklar och certifikat. Märkningen anger vilken signalskyddsgrad en viss nyckelserie eller certifikat är godkänd för samt ger vägledning avseende krav på hantering och förvaring.

Signalskyddssystemets faktiska styrka vid användandet avgörs dels av signalskyddssystemets maximala styrka, dels av signalskyddsnyckelns märkning. Den faktiska signalskyddsgraden är den lägsta av signalskyddssystemets maximala styrka och signalskyddsnyckelns märkning.

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.

En signalskyddsinstruktion ska beskriva de faktiska förhållandena där signalskyddsverksamheten bedrivs. Den ska vara ett stöd till verksamheten och ge relevant information och vägledning till all personal som kommer i kontakt med eller är i behov av signalskydd.

Signalskyddsinstruktionen i sin helhet måste inte delges alla som bedriver signalskyddstjänst, det viktiga är att rätt information når rätt personer.

Exempel på uppdelning kan vara att allmänna regler och rutiner som berör alla som kommer i kontakt med signalskydd delges samtliga emedan beskrivningar av rutiner och arbetsuppgifter som endast berör signalskyddspersonal endast delges dessa.

Tillämpliga delar kan vara utdrag ur signalskyddsinstruktionen eller ännu hellre sammanfattningar i bilagor som beskriver de rutiner och åtgärder som behöver vidtas och följas för respektive kategori signalskyddspersonal, användare, NaV-handläggare och övrig personal.

En signalskyddsinstruktion ska bevaras och det är därför inte lämpligt att en

signalskyddsinstruktion innehåller registeruppgifter eller andra uppgifter som ofta förändras. Register som omfattar verksamhetsutövarens samtliga nycklar, materiel, aktiva kort, certifikat och personal ska hållas aktuella. Registrens innehåll och omfattning gör att de bör omfattas av sekretess och ska endast delges personal som behöver uppgifterna för sin tjänst.