Nasjonal sikkerhetsmyndighet

Veiledning

Sist oppdatert: 2007-04-19

Veiledning i administrativ kryptosikkerhet

Kapittel 7 i Forskrift om informasjonssikkerhet, som omhandler administrativ kryptosikkerhet, er omfattende og detaljrik. Imidlertid er det forhold knyttet til den enkelte paragraf som ikke er selvforklarende. I denne veiledningen er derfor forskriften forklart og utdypet paragraf for paragraf. Vedleggene til veiledningen er maler og skjemaer, som vil være en støtte i utøvelsen av administrativ kryptosikkerhet.

Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet er tverrsektoriell fag- og tilsynsmyndighet innenfor forebyggende sikkerhetstjeneste i Norge og forvalter lov om forebyggende sikkerhet av 20 mars 1998. Hensikten med forebyggende sikkerhet er å motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, primært spionasje, sabotasje og terrorhandlinger. Forebyggende sikkerhetstiltak skal ikke være mer inngripende enn strengt nødvendig, og skal bidra til et robust og sikkert samfunn.

Hensikt med veiledning

NSM sin veiledningsvirksomhet skal bygge kompetanse og øke sikkerhetsnivået i virksomhetene, gjennom økt motivasjon, evne og vilje til å gjennomføre sikkerhetstiltak. NSM gir jevnlig ut veiledninger til hjelp for implementering av de krav sikkerhetsloven stiller. NSM publiserer også veiledninger innen andre fagområder relatert til forebyggende sikkerhetsarbeid.

Postadresse
Postboks 14
1306 BÆRUM
POSTTERMINAL

Sivil telefon/telefax
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
post@nsm.stat.no

Militær telefon/telefaks
515 40 00/515 40 09

Internettadresse
www.nsm.stat.no

Innhold

1 Innledning 4
1.1 Bakgrunn 4
1.2 Hensikt 4
1.3 Referanser 4
2 Generelt om Forskriftens forhold til NATOs bestemmelser om kryptosikkerhet. 5
3 B. Myndighet, oppgaver og organisering innen administrativ kryptosikkerhet 5
3.1 Til § 7-1. Anvendelsesområde, motstrid og dispensasjon 5
3.2 Til § 7-2 NSMs myndighet og oppgaver innen kryptosikkerhet 5
3.3 Til § 7-3 Hovedforvalters ansvar for kryptoutstyr 7
3.4 Til § 7-4 Overordnet virksomhets ansvar for underordnet virksomhet. 7
3.5 Til § 7-5 Virksomhet som leverer kryptosikkerhetstjenester eller produserer kryptoutstyr 7
3.6 Til § 7-6 Plikt til å etablere kryptosikkerhetsorganisasjon 8
3.7 Til § 7-7 Virksomhetens leder 8
3.8 Til § 7-8 Kryptosikkerhetsleder 9
3.9 Til § 7-9 Kryptoforvalter 10
3.10 Til § 7-10 Kryptobruker 12
3.11 Til § 7-11 Utdanning av kryptopersonell 13
4 C. Kryptoautorisasjon og kryptokvalifisering 13
4.1 Til § 7-12 Kryptoautorisasjon 13
4.2 Til § 7-13 Kryptokvalifiserende myndighet 14
4.3 Til § 7-14 Krav til kryptokvalifisering grad 2 14
5 D. Distribusjon og forvaltning av kryptomateriell 14
5.1 Til § 7-15. Krav til kryptokvalifisering grad 1 14
5.2 Til § 7-16. Tilbakekallelse av kryptokvalifisering 15
D. Distribusjon og forvaltning av kryptomateriell 15
5.3 Til § 7-17 Klassifisering og merking 15
5.4 Til § 7-18 Distribusjon av kryptomateriell 16
5.5 Til § 7-19 Forsendelse 17
6 E. Kryptoregnskap 17
6.1 Til § 7-20 Etablering av kryptoregnskap 17
6.2 Til § 7-21 Føring av kryptoregnskap 18
6.3 Til § 7-22. Regnskapskoder 18
6.4 Til § 7-23. Mottak og utlån av kryptomateriell 19
6.5 Til § 7-24 Mangfoldiggjøring 19
6.6 Til § 7-25 Rapportering 20
6.7 Til § 7-26 Sikkerhetsgradering av regnskap og rapporter 21
6.8 Til § 7-27. Kontroll av beholdning 21
6.9 Til § 7-28 Avslutning av kryptoregnskap 21
7 F. Tilintetgjøring. 22
7.1 Til § 7-29 Tilintetgjøring av kryptonøkler 22
7.2 Til § 7-30. Tilintetgjøring av kryptodokumenter 22
7.3 Til § 7-31. Krav til personell som forestår tilintetgjøring 22
7.4 Til § 7-32. Metoder for tilintetgjøring 23
7.5 Til § 7-33 Tilintetgjøringsrapport 23
7.6 Til § 7-34. Evakuering og ekstraordinær tilintetgjøring 23
8 G. Fysisk sikring. 23
8.1 Til § 7- 35 Sikring av kryptomateriell 23
8.2 Til § 7-36. Sikring av kryptorom 24
8.3 Til § 7-37 Adgangskontroll 24
8.4 Til § 7-38. Oppbevaring 25
8.5 Til § 7-39 Låser og nøkler 25
8.6 Til § 7-40 Installasjon av kryptoutstyr 25
9 H. Reaksjon ved sikkerhetstruende hendelser 26
9.1 Til § 7-41. Typer sikkerhetstruende hendelser 26
9.2 Til § 7-42. Generelt om rapporterings- og tiltaksplikt 27
9.3 Til § 7-43 Nærmere om rapportering 27

9.4 Til § 7-44 Adressater for rapportering av nasjonalt materiell 28
9.5 Til § 7-45 Adressater for rapportering av NATO materiell 28
Vedlegg A Dokumenthistorie – (Obligatorisk) 28

1 Innledning

1.1 Bakgrunn

Det er et behov for utdyping av forskriftene knyttet til administrativ kryptosikkerhet.

1.2 Hensikt

Hensikten med veiledningen er å bidra til at kravene til administrativ kryptosikkerhet blir lettere å forstå og derved enklere å etterleve.

1.3 Referanser

Lov om Forebyggende sikkerhetstjeneste

Forskrift om informasjonssikkerhet kapittel 7

AMSG 293

2 Generelt om Forskriftens forhold til NATOs bestemmelser om kryptosikkerhet.

Innholdet i forskriften er stort sett lik NATO`s bestemmelser, selv om strukturen og noe av terminologien fremstår som forskjellig. Der bestemmelsene avviker fra NATOs krav gir forskriften strengere krav til sikkerhet. Forskriften kan derfor anvendes til å behandle NATOs kryptomateriell slik at håndteringen blir enklere for de som forvalter begge typer informasjon. Dette er særlig aktuelt der nasjonalt og NATO kryptomateriell håndteres i samme systemer. I tillegg gjør overgangen fra typiske militære begreper til mer allmenngyldige begreper, samt forskriftenes norske språk, at regelverket blir lettere tilgjengelig.

Alle virksomheter som har NATO kryptomateriell gjelder bestemmelsene gitt i NATO publikasjon AMSG 293 gjeldende utgave, i tillegg til bestemmelsene gitt i C-M (2002)49. Der hvor bestemmelsene er forskjellige gjelder Forskrift om administrativ kryptosikkerhet.

Forskrift om Informasjonssikkerhet kapittel 7 pkt H "Reaksjon ved sikkerhetstruende hendelser" gir krav som er spesielle for kryptosikkerhet. For krypto gjelder altså ikke bestemmelsene vedrørende sikkerhetstruende hendelser i kap 5 i Forskrift om sikkerhetsadministrasjon. Begrunnelsen er spesielle distribusjonskanaler og kravet til hurtig rapportering innen kryptosikkerhet. I tillegg kommer NATOs regler om rapportering til anvendelse (AMSG 293). Forskriftens kapittel 7 ivaretar NATOs krav til kryptosikkerhet.

Vedleggene til veiledningene er et godt hjelpemiddel i det daglige arbeidet med kryptosikkerhet.

3 B. Myndighet, oppgaver og organisering innen administrativ kryptosikkerhet

3.1 Til § 7-1. Anvendelsesområde, motstrid og dispensasjon

§ 4-18 til § 4-35 gjelder ikke for kryptodokumenter som er gitt regnskapskode (RK) eller merket KRYPTO eller NSK. § 4-19 femte ledd og § 4-31 gjelder likevel.

Ved motstrid mellom bestemmelser i kapittel 6 og § 7-36 til § 7-41 går § 7-36 til § 7-41 foran.

NSM kan dispensere fra første ledd i § 7-14, § 7-15 og § 7-27, og § 7-29, § 7-30 andre ledd, § 7-33 fjerde ledd og § 7-36 til § 7-41.

3.2 Til § 7-2 NSMs myndighet og oppgaver innen kryptosikkerhet

Forskrift om informasjonssikkerhet gir bestemmelser om NSM sin rolle innen kryptosikkerhet. Den er en sentral hjemmel for NSMs myndighetsutøvelse på området.

Distribusjon av kryptomateriell er nærmere beskrevet i § 7-18.

NSM er nasjonal distribusjonsmyndighet for kryptomateriell med ansvar for distribusjon av kryptomateriell og kontroll med regnskap, og « National Distributing Authority Norway (NDA) » i forhold til NATO.

NSM er leverandør av kryptosikkerhetstjenester til utenrikstjenesten, Politiets overvåkingstjeneste, Forsvaret og i forbindelse med den kommunikasjon virksomheter med totalforsvarsoppgaver må ha med Fsorsvaret av beredskapsmessige hensyn. NSM kan dispensere fra bestemmelsene i dette leddet.

NSM skal produsere kryptonøkler og utgi kryptodokumenter.

NSM skal utpeke virksomheter med myndighet til å gi kryptokvalifisering, jf. § 7-13 til § 7-16, og hovedforvalter for hver type kryptoutstyr.

NSM har gitt andre virksomheter kryptokvalifiserende myndighet ref vedlegg.

NSM har utpekt hovedforvaltere for alt kryptoutstyr ref vedlegg.

NSM skal produsere kryptonøkler og utgi kryptodokumenter.

Følgende skal godkjennes av NSM:

1. *Kryptoutstyr, herunder NSK, til beskyttelse av sikkerhetsgradert informasjon. Formidles informasjon sikkerhetsgradert NATO SECRET eller COSMIC TOP SECRET, skal kryptosystemet i tillegg være godkjent av NATO. Informasjon merket ATOMAL, STRENGT HEMMELIG, KRYPTO, EKSKLUSIV eller tilsvarende skal behandles på separate systemer godkjent av NSM.*

2. *Anskaffelse av kryptomateriell for beskyttelse av sikkerhetsgradert informasjon.*

3. *Bruk av kryptoutstyr og kryptosystemer, og kryptosikkerheten i den enkelte virksomhet før virksomheten kan ta kryptomateriell i bruk.*

4. *Andre virksomheter enn NSM som skal levere kryptosikkerhetstjenester, herunder tredjepart for offentlige systemer for fordeling av kryptonøkler.*

5. *Virksomheter som skal utvikle kryptoutstyr.*

6. *Andre virksomheter som skal produsere kryptonøkler og kryptodokument. NSM bestemmer type av kryptonøkler og gyldighetsperiode for disse.*

Bare kryptoutstyr godkjent av NSM kan benyttes til sikring av skjermingsverdig informasjon, dette er av prinsipiell betydning og utledet av Sikkerhetslovens § 14.

Bare godkjente leverandører av kryptosikkerhetstjenester kan tilby godkjent kryptoutstyr, ref 2.4 i denne veiledningen.

Dersom NSM godkjenner virksomhet som nevnt i femte ledd nr. 4 til 6, skal NSM inngå avtale med virksomheten om ansvar og sikkerhetsmessige forhold.

Oversikt over godkjent nasjonalt kryptoutstyr skal utgis av NSM. Oversikt over NATO-godkjent kryptoutstyr utgis av NATO Distribution and Accounting Agency (DACAN).

NSM skal kontrollere at bestemmelsene i denne forskrift følges. Periodiske inspeksjoner for dette formål skal foretas. Rapport fra inspeksjon skal

oppbevares i minst fem år hos NSM, den inspiserte virksomheten og eventuelt overordnet virksomhet.

I vedlegg er det gitt forslag til kontrollskjema for inspeksjoner/egenkontroll.

Kontrollskjemaet inneholder de punktene NSM kontrollerer i forbindelse med kryptosikkerhetsinspeksjoner.

3.3 Til § 7-3 Hovedforvalters ansvar for kryptoutstyr

Hovedforvalter er ansvarlig for kryptoutstyret gjennom hele dets levetid, herunder for reparasjon, vedlikehold, avhending og utgivelse av tekniske håndbøker.

Vedlegg[B] viser hvem som er hovedforvalter for det enkelte kryptoutstyret.

3.4 Til § 7-4 Overordnet virksomhets ansvar for underordnet virksomhet.

Overordnet virksomhet skal kontrollere at bestemmelsene i denne forskrift følges av underordnet virksomhet. Periodiske inspeksjoner for dette formål skal foretas. Rapport fra inspeksjon skal oppbevares i minst fem år ved NSM, den inspiserende virksomhet og den inspiserte virksomhet.

Vedlegg er et forslag til kontrollskjema for bruk i forbindelse med inspeksjoner.

Betegnelsen overordnet virksomhet vil i denne forbindelse være eksempelvis:

- Forsvarets Sikkerhetsavdeling for Forsvarets avdelinger.
- Direktoratet for samfunnssikkerhet og beredskap for Fylkesmennene, Fylkeskommuner og kommuner.
- Utenriksdepartementet for utenriksstasjoner.
- Politidirektoratet for Politiet.

3.5 Til § 7-5 Virksomhet som leverer kryptosikkerhetstjenester eller produserer kryptoutstyr

Virksomhet som skal levere kryptosikkerhetstjenester i samsvar med sikkerhetsloven § 14 andre ledd andre punktum er ansvarlig for salg, utleie, installasjon og drift av kryptoutstyr, og for administrasjon av kryptonøkler. Virksomheten skal føre kontroll med kryptosikkerheten hos brukerne. Virksomhet som ikke er forvaltningsorgan skal være leverandørklarert for den høyeste sikkerhetsgradering av kryptonøkler som blir levert, likevel for minst KONFIDENSIELT.

Ved produksjon av kryptonøkler gradert KONFIDENSIELT eller HEMMELIG skal involvert personell ha kryptokvalifisering grad 1.

Lokaliteter hvor det utføres administrasjon av kryptonøkler og drift av kryptoutstyr skal være fysisk sikret for den høyeste sikkerhetsgrad kryptonøklene har og minst som for KONFIDENSIELT.

Virksomhet som ikke er forvaltningsorgan og skal produsere kryptoutstyr hvor kryptoalgoritmer til NATO eller NSK inngår, skal på forhånd være leverandørklarert for HEMMELIG eller høyere.

Hva et forvaltningsorgan i medhold av Sikkerhetsloven er, går frem av Sikkerhetslovens § 2.

Følgende virksomheter kan tilby kryptoutstyr godkjent av NSM:

- NSM
- ERGO Group
- Kongsberg Defence Aerospace (KDA)
- Thales Communications Norway

3.6 Til § 7-6 Plikt til å etablere kryptosikkerhetsorganisasjon

Virksomhet som besitter kryptomateriell skal etablere en kryptosikkerhetsorganisasjon med kryptosikkerhetsleder og kryptoforvalter med stedfortredere, og etablere ordning for henting og levering av kryptomateriell med kurerpost.

Det skal etableres en hensiktsmessig kurertjeneste. Innenlands må det opprettes et samarbeid mot Forsvarets kurertjeneste (FOKS) tlf 23 09 89 70/89 81 og for utlandet med Utenriksdepartementet (UD) tlf 22 24 30 58 eller mot FOKS (NATO).

Virksomheten må selv ta initiativ for å etablere hensiktsmessige distribusjonskanaler.

Kryptosikkerhetspersonellet skal være faglig kvalifisert, herunder kryptokvalifisert, ha nødvendig myndighet i virksomheten og kunne ivareta funksjonen i minst ett år. Personellet skal ikke pålegges andre oppgaver i den utstrekning det fratar dem muligheten til å ivareta funksjonen i samsvar med gjeldende sikkerhetsbestemmelser. Bare personell som har vært fast ansatt i virksomheten i minst ett år kan utpekes til kryptosikkerhetsleder eller kryptoforvalter, med mindre NSM i det enkelte tilfelle samtykker i annet.

Med faglig kvalifisert menes også nødvendige ferdigheter i betjening av virksomhetens kryptoutstyr. Virksomheten er selv ansvarlig for å gi den enkelte opplæring i bruk av kryptoutstyret. Forsvarets skoler arrangerer kurs på de fleste utstyrstyper, ref vedlegg.

3.7 Til § 7-7 Virksomhetens leder

Virksomhetens leder er ansvarlig for at sikkerhetsbestemmelsene for kryptotjenesten blir fulgt i egen virksomhet, herunder:

1. *Skriftlig utpeke kryptosikkerhetsleder og kryptoforvalter med stedfortredere.*

2. *Minimum en gang i året kontrollere utførelsen av kryptosikkerhetstjenesten.*

3. *Iverksette nødvendige tiltak for å redusere skadevirkning og rapportere til overordnet virksomhet ved sikkerhetsbrudd, kompromittering, uautorisert endring eller utilgjengelighet av kryptoutstyr eller sikkerhetsgradert informasjon.*

4. *Snarest rapportere til NSM og klareringsmyndighet i tilfeller av fjerning eller uautorisert fravær av kryptoforvalter eller stedfortreder, og om nødvendig utpeke ny kryptoforvalter eller stedfortreder.*

Skjema i vedlegg brukes ved utnevningen av kryptosikkerhetsleder og kryptoforvalter med stedfortredere. Et eksemplar av skjemaet skal til eget arkiv og et til overordnet distribusjonsmyndighet. Overordnet distribusjonsmyndighet vil for Utenrikstjenesten være UD, for sivil statsforvaltning NSM og for Forsvaret nærmeste overordnede distribusjonsledd. Alle eksemplarer skal være original, dvs ha originale signaturer. NSM skal ha et eksemplar av utnevnelsen fra alle overordnede kryptodistribusjonsledd.

På grunn av kryptomateriellets sårbarhet, og strenge kontrollkrav må kryptoforvalter og stedfortreder være pålitelige og utvise stor grad av nøyaktighet. Det er derfor nødvendig at virksomhetens leder er nøye med å velge ut kvalifisert personell som:

1. Er i en stilling som gir vedkommende den nødvendige autoritet i virksomheten (viktig for å kunne gi dette arbeidet tilstrekkelig prioritet).

2. Er motivert for å ta på seg dette ansvarsfulle og tidkrevende arbeidet. Dette er ofte et biarbeid som krever mye. Interesse for forebyggende sikkerhet og sambandstjeneste er derfor viktig å ta hensyn til ved utvelgelse av personellet.

3. Ikke tidligere har blitt avløst som kryptoforvalter på grunn av skjødesløshet eller manglende utførelse av sine plikter.

Administrativ kryptosikkerhet er preget av rutiner, men med varierende arbeidsbelastning. Det er derfor avgjørende at kryptosikkerhetspersonellet, til enhver tid, får mulighet til å ivareta sitt ansvar og sine funksjoner i samsvar med gjeldende sikkerhetsbestemmelser. Er ikke dette mulig/vanskelig å gjennomføre, plikter virksomhetens leder å rapportere til overordnet virksomhet og NSM.

Personell utpekt i funksjonene skal være sikkerhetsklarert, kryptokvalifisert og autorisert jf §§ 7-14 – 7-15 for det kryptomateriell de er satt til å forvalte.

3.8 Til § 7-8 Kryptosikkerhetsleder

Kryptosikkerhetsleder skal føre daglig tilsyn med at sikkerhetsbestemmelsene for kryptotjenesten blir fulgt, herunder:

1. *Sørge for opplæring av personell som arbeider med kryptomateriell slik at de er kjent med instruksene til kryptoutstyr som er i bruk.*

2. *Gjøre virksomhetens leder oppmerksom på sikkerhetsgradert informasjon som er sendt eller mottatt i et kryptosystem som av kontrollerende myndighet er erklært kompromittert, uautorisert endret eller utilgjengelig.*

3. *Øyeblikkelig rapportere til virksomhetens leder enhver kjent eller mulig kompromittering, tap, uautorisert tilintetgjøring eller utilfredsstillende oppbevaring av kryptomateriell.*

4. *Utarbeide plan for tilintetgjøring og evakuering av kryptomateriell i samsvar med § 7-34 og sørge for at nødvendig utstyr er tilgjengelig for å gjennomføre planen.*

5. *Utarbeide lokal kryptosikkerhetsinstruks som skal godkjennes av virksomhetens leder, og etablere lokale løsninger og prosedyrer for krav angitt i lov eller forskrift skal følges.*

Kryptosikkerhetsleder er lederens rådgiver i alle spørsmål angående kryptosikkerhet, fysisk sikring av kryptomateriell, intern kontroll og implementering av alle andre sikkerhetstiltak relatert til kryptotjenesten. Om arbeidssituasjonen gjør det vanskelig å gjennomføre kryptosikkerhetstjenesten i samsvar med gjeldende sikkerhetsbestemmelser skal kryptosikkerhetsleder umiddelbart ta dette opp med virksomhetens leder.

Kryptosikkerhetsleder er pålagt følgende plikter for å *oppnå en sikker*, nøyaktig og effektiv kryptotjeneste:

1. Utarbeide lokal kryptosikkerhetsinstruks, se vedlegg. Instruksen skal være tilpasset lokale forhold, slik at den er et verktøy i det daglige arbeidet med administrativ kryptosikkerhet.
2. Kontrollere at personell får tilstrekkelig rettledning og trening på kryptosystemene de skal operere. Nytt personell skal gjøres kjent med lokale instrukser/rutiner. Personellet skal årlig kvittere for gjennomlesing av instruksene, se vedlegg.
3. Utarbeide retningslinjer og prosedyrer for hvordan meldinger skal behandles. Det må opprettes en journal for INN- og UT-meldinger i virksomhetens kryptosystemer. Journalen skal inneholde nødvendige detaljer om hver enkelt melding, se vedlegg[i].

   INN- og UT-meldinger i kryptosystemer er å betrakte som dokumenter, og skal behandles i samsvar med Forskrift om informasjonssikkerhet kapittel 4.
4. Gi råd til utstedere av meldinger angående utstederrett, bruk av prioriteter og sikkerhetsgradering der dette synes nødvendig.
5. Kontrollere at bare det personellet som er autorisert skal ha adgang til ”spesiell kategori meldinger” (SPECAT-meldinger) og SPECAT nøkkelmateriell. Det skal utarbeides en egen instruks for behandling av SPECAT-meldinger.
6. Kontrollere at gradert materiell og alt kryptomateriell til enhver tid blir forskriftsmessig behandlet og oppbevart.
7. Kontrollere at kryptoutstyr blir forskriftsmessig vedlikeholdt, og at det virker som det skal. Hovedforvalter er ansvarlig for vedlikehold av kryptoutstyr, se vedlegg.
8. Sørge for at brudd på fysisk sikkerhet og kryptosikkerhet øyeblikkelig blir rapportert iht bestemmelsene i kapittel 7 H.
9. Utarbeide instruks for rutinemakulering av kryptomateriell.
10. Å utarbeide en skriftlig nødmakuleringsplan og sørge for at personellet er kjent med og trent i planen. Videre sikre at nødvendig utstyr er tilgjengelig for å utføre planen iht bestemmelsene i kapittel 7 F.
11. Kryptosikkerhetsleder skal i samarbeid med virksomhetens leder rapportere til overordnet myndighet og NSM enhver kompromittering av sikkerhetsgradert informasjon. Enhver kompromittert melding som inneholder kryptoinformasjon skal rapporteres som angitt i kapittel 7 H.

3.9 Til § 7-9 Kryptoforvalter

Kryptoforvalter skal forvalte kryptomateriell ved virksomheten, herunder:

1. *Motta, oppbevare og behandle alt kryptomateriell for å hindre tap og kompromittering.*

2. *Føre løpende kryptoregnskap over kryptomateriell og ha kontroll med hvor regnskapspliktig kryptomateriell befinner seg og hva det brukes til.*

3. *Utføre tilintetgjøring og sende tilintetgjøringsrapport i samsvar med pålagte krav.*

4. *Distribuere eller overføre kryptomateriell til autoriserte brukere.*

5. *Gjøre seg kjent med gjeldende planer for tilintetgjøring, evakuering og beskyttelse av kryptomateriell i tilfelle brann eller andre nødsituasjoner.*

6. *Etablere prosedyrer for å sikre kontroll med kryptonøkler og annet kryptomateriell som skal overbringes fra en person til en annen.*

7. *Øyeblikkelig rapportere til virksomhetens leder eller kryptosikkerhetsleder enhver kjent eller mulig kompromittering, tap, uautorisert tilintetgjøring eller utilfredsstillende oppbevaring av kryptomateriell.*

Stedfortredende kryptoforvalter skal bistå kryptoforvalter i utførelsen av dennes oppgaver, og i dennes fravær overta ansvar og gjøremål. Stedfortredende kryptoforvalter har ikke ansvar for kryptomateriell når kryptoforvalter er til stede.

1. Sikring og oppbevaring av kryptomateriell er behandlet i Forskriftens kapittel 7 G. Kryptoforvalter skal forsikre seg om at alle som får overdratt kryptomateriell, kan behandle og oppbevare dette i samsvar med gjeldende sikkerhetsbestemmelser.

2. Kryptoforvalter skal føre kryptoregnskap med tilhørende bilag, og regnskapet skal være ajour til en hver tid. Det innebærer at alle transaksjoner uten ubegrunnet opphold skal registreres i regnskapet. Overføringspapirer skal returneres overordnet distribusjonsmyndighet innen 48 timer. Regnskapet skal omfatte alt kryptomateriell, samt angi hvor materiellet befinner seg. I vedlegg er det gitt eksempel på hvordan et kryptoregnskap skal føres. Brukere av systemene EKNAS/BRIS 2 skal…

   Holdere av kryptomateriell skal ikke benytte beholdningsoppgave tilsendt fra overordnet distribusjonsmyndighet som kryptoregnskap.

   Kryptoforvalter skal forberede og sende alle påbudte regnskapsrapporter innen tidsfristene gitt i veiledningens punkt 5.4.

   Det er kryptoforvalters oppgave å påse at kryptobeholdningen er i samsvar med behovet. Overflødig materiell skal avbestilles…

   Når det er behov for nytt kryptomateriell er det kryptoforvalters oppgave å bestille dette iht krav gitt i Forskriftens § 7-18.

   Kryptoforvalter skal foreta fysisk kontroll av alt kryptomateriell,

   ref Forskriftens § 7-27.

   KRYPTOREGNSKAPET SKAL HA GRADERINGEN K O N F I D E N S I E L T

3. Makuleringsrapporter skal være overordnet distribusjonsmyndighet i hende før den 15. i hver måned. For detaljer vedrørende tilintetgjøring, se Forskriften kapittel 7 F.

4. Rutinemessig opptelling av kryptobeholdningen er en forutsetning for god kontroll med kryptomateriellet. NSM anbefaler at full opptelling minimum blir gjennomført hvert kvartal.

5. Kryptoforvalter skal forsikre seg om at alle mottakere av kryptomateriell er sikkerhetsklarert, kryptokvalifisert og autorisert.

6. Kryptoforvalter skal til enhver tid holde seg orientert om gjeldende instrukser for kryptotjenesten. Kryptoforvalter bør årlig øve gjennomføring av plan for nødmakulering og evakuering. Foretas det endringer i planverket, skal gjennomførbarheten kontrolleres gjennom en øvelse.

7. Ved intern overføring av kryptomateriell til kryptobruker, skal det skrives håndkvittering. Kryptoregnskapet må umiddelbart ajourføres. Det er ikke tillatt å overføre materiellet til tredje part! Flere detaljer om intern overføring er gitt i vedlegg[ii].

8. NSM understreker viktigheten av umiddelbar rapportering av kompromitteringer eller mulige kompromitteringer. Årsaken til dette er at kontrollerende myndighet kan treffe nødvendige tiltak, for å sikre integriteten og konfidensialiteten til skjermingsverdig informasjon.

9. Spesielle retningslinjer for brukere av EKNAS/NOR er å finne i vedlegg.

Ved fravær over 60 dager skal ny kryptoforvalter utpekes.

Stedfortredende kryptoforvalter må være godt kjent med kryptoforvalters plikter og gjøremål, for å kunne overta oppgaven som kryptoforvalter i dennes fravær.

Etter et midlertidig fravær skal kryptoforvalter informeres av sin stedfortreder om alle forandringer i regnskapet. Er kryptomateriell overført eller tilintetgjort skal kryptoforvalter kontrollere dette har skjedd korrekt ved å sammenligne overførselen eller tilintetgjøringsrapporten med regnskapet.

Ved skifte av kryptoforvalter skal fratredende og tiltredende kryptoforvalter foreta opptelling av alt registrert kryptomateriell i samsvar med regnskapet. Ved større virksomheter kan kontrollgrupper bistå i utførelsen av kontrollen under ledelse av kryptoforvalter. Fra- og tiltredende kryptoforvalter skal utferdige beholdningsoppgave som skal merkes « bytte av kryptoforvalter » og inneholde alt registrert kryptomateriell tiltredende kryptoforvalter blir ansvarlig for. Signert kopi av beholdningsoppgaven skal beholdes i lokalt regnskap og i tillegg sendes distribusjonsmyndigheten.

Etter å ha kvittert for kryptomateriellet har den nye kryptoforvalter ansvar for regnskapet. Ved mangler eller misligheter i kryptoregnskapet er likevel fratredende kryptoforvalter fortsatt ansvarlig inntil disse er rettet.

Virksomhetens leder skal i god tid før kryptoforvalter slutter utpeke en avløser.

Opplæring og eventuell kursing skal være gjennomført før overtagelse.

Avtroppende- og påtroppende- kryptoforvalter skal telle opp alt kryptomateriell (overtagelsesforretning). Avtroppende kryptoforvalter er ansvarlig for eventuelle feil og mangler som blir avdekket under opptellingen.

3.10 Til § 7-10 Kryptobruker

Bruker av kryptomateriell skal følge gjeldende bestemmelser for bruk, oppbevaring og tilintetgjøring av materiellet.

Kryptobruker skal ha gjennomført opplæring i bruk av tildelt kryptomateriell, samt være kjent med de instrukser som gjelder for materiellet. Kryptobruker skal være sikkerhetsklarert, kryptokvalifisert og kryptoautorisert. Vedkommende skal også være kjent med virksomhetens lokale sikkerhetsinstruks.

3.11 Til § 7-11 Utdanning av kryptopersonell

Kryptokvalifiserende myndighet skal gi generell opplæring i kryptosikkerhet for personell som skal ha tilgang til kryptomateriell og informasjon om sikkerhet ved kryptotjenesten.

I vedlegg er det listet kryptokvalifiserende myndigheter, og virksomheter som kan gjennomføre utdanning innen kryptotjenesten.

Den enkelte virksomhet skal sørge for at operatører får opplæring i bruk av aktuelt kryptoutstyr.

Hovedforvalter skal sørge for opplæring av personell som skal utføre teknisk vedlikehold eller reparasjon av kryptoutstyr.

Hovedforvalter er ansvarlig for at teknisk personell får nødvendig opplæring/utdanning. Opplæringen gjennomføres vanligvis i regi av leverandøren av utstyret, eller ved utdanningsinstitusjoner med nødvendig kompetanse.

I prosjekter for anskaffelse av nytt kryptoutstyr anbefaler NSM at utdanning inngår som en del av prosjektet.

Leverandør av kryptosikkerhetstjenester skal i nødvendig utstrekning bistå i opplæringen.

NSM skal godkjenne programmer for opplæring nevnt i første og andre ledd. Opplæringsprogram for kryptosikkerhet skal revideres ved behov og minst hvert annet år. Uavhengig av endringer skal programmer fremsendes til NSM for godkjenning.

4 C. Kryptoautorisasjon og kryptokvalifisering

4.1 Til § 7-12 Kryptoautorisasjon

For tilgang til kryptomateriell uten manipuleringssikring godkjent av NSM eller informasjon merket KRYPTO kreves kryptoautorisasjon. Kravet til kryptoautorisasjon gjelder i tillegg til krav om sikkerhetsklarering og autorisasjon etter de alminnelige bestemmelser for personellsikkerhet.

Personellet skal være kryptoautorisert for å kunne håndtere det materiellet de har i sin besittelse. Det er viktig at personellet ikke blir autorisert for tilgang til kryptomateriell de ikke er kvalifisert for §§ 7-14 – 7-15.

Kryptoautorisasjon kan gis av virksomhetens leder når sikkerhetsklarering og kryptokvalifisering foreligger. Ved utenlandstjeneste kan bare personell med diplomatisk status eller militært personell kryptoautoriseres, med mindre NSM samtykker i annet i det enkelte tilfelle. Blankett godkjent av NSM skal benyttes ved kryptoautoriseringen. Virksomheten skal føre oversikt over eget kryptoautorisert personell.

Blankett for kryptoautorisasjon er tilgjengelig i vedlegg.

Autorisasjonsliste er tilgjengelig i vedlegg.

Virksomhetens leder behøver ikke kryptokvalifisering for å utøve kontroll i samsvar med § 7-7 nr. 2. Leder som ikke er kryptokvalifisert skal ikke ha tilgang til kryptonøkler i klartekst.

4.2 Til § 7-13 Kryptokvalifiserende myndighet

Kryptokvalifisering gis av NSM eller virksomhet som NSM utpeker.

4.3 Til § 7-14 Krav til kryptokvalifisering grad 2

Kryptokvalifisering grad 2 kan bare gis når personellet har tjenstlig behov, har sikkerhetsklarering for HEMMELIG/tilsvarende eller høyere, er norsk statsborger og har gjennomført opplæring som nevnt i § 7-11 første ledd.

Tjenstlig behov etter første ledd foreligger bare dersom det er nødvendig å gi personell tilgang til

1. *kryptonøkler for testformål eller operativ bruk gradert til og med HEMMELIG,*

2. *å kryptere eller dekryptere mellom to forbindelsespunkter,*

Kryptering og dekryptering mellom to forbindelsespunkter, dvs to punkt til punkt forbindelser eller en forbindelse som involverer Managementcenter.

Personell som håndterer kryptomateriell utover dette skal være kryptokvalifisert grad I, ref § 7-15.

3. *informasjon merket KRYPTO, eller*

4. *kryptoutstyr for det formål å reparere eller vedlikeholde utstyret.*

5 D. Distribusjon og forvaltning av kryptomateriell

5.1 Til § 7-15. Krav til kryptokvalifisering grad 1

Kryptokvalifisering grad 1 kan bare gis når personellet har tjenstlig behov, har sikkerhetsklarering for STRENGT HEMMELIG/tilsvarende, er norsk statsborger og har gjennomført opplæring som nevnt i § 7-11 første ledd.

Tjenstlig behov etter første ledd foreligger bare dersom det er nødvendig å gi personell tilgang til

1. *kryptonøkler sikkerhetsgradert STRENGT HEMMELIG,*

2. *kryptonøkler for kryptering og dekryptering mellom flere enn to forbindelsespunkter,*

3. *å produsere kryptonøkler, eller*

4. *å operere kryptosystem godkjent for ATOMAL, STRENGT HEMMELIG, KRYPTO, EKSKLUSIV*

eller tilsvarende.

5.2 Til § 7-16. Tilbakekallelse av kryptokvalifisering

NSM eller kryptokvalifiserende myndighet kan tilbakekalle en kryptokvalifisering gitt til person som ikke lenger har tilfredsstillende kunnskaper eller ferdigheter i kryptosikkerhet. NSM skal umiddelbart underrettes om tilbakekallingen.

Sikkerhetsloven § 24 gjelder for kryptoautorisasjon så langt den passer.

D. Distribusjon og forvaltning av kryptomateriell

5.3 Til § 7-17 Klassifisering og merking

Kryptomateriell skal identifiseres med en langtittel som beskriver innholdet eller utstyret, og en korttittel som skal brukes for regnskapsføring. Kryptomateriell kan også identifiseres med et annet navn enn korttittel. Korttittel eller annet navn bestemmes og tildeles av NSM. Individuell korttittel skal være ugradert. Langtittelen sikkerhetsgraderes etter sitt innhold.

Ved nyanskaffelse skal anskaffelsesmyndigheten avklare med NSM hvordan materiellet skal klassifiseres og merkes.

Produsent av kryptoutstyr og kryptonøkler skal påføre et entydig registreringsnummer.

Når kryptomateriell er merket med serienummer brukes dette normalt som registreringsnummer i kryptoregnskapet. Dersom det oppstår tvil om dette, skal NSM avgjøre hva som skal brukes som registreringsnummer.

I tillegg til identifikasjon med langtittel, korttittel og registreringsnummer, kan kryptomateriell identifiseres med alfabetiske eller numeriske utgaver.

Alfabetisk eller numerisk merking brukes for å skille mellom ulike utgaver av kryptomateriell med samme tittel, feks. på kryptonøkler, publikasjoner, utstyr, osv. Utgavemerking brukes også for å identifisere effektiv kryptoperiode for krypto nøkkelmateriell i henhold til utgitte publikasjoner (NMSG 30 for nasjonalt kryptomateriell og AMSG 600 for NATO kryptomateriell). Slik informasjon kan også være meddelt på annen måte av overordnet myndighet.

Eksempel: NMST 502 AAK (Kort tittel: NMST 502, utgave: AAK)

Informasjon om kryptonøkler, kryptoalgoritmer, sikkerhetsspesifikasjoner om kryptosystemer og detaljer som omhandler egenskaper til kryptosystemer, skal merkes KRYPTO. Dette omfatter blant annet diagrammer og fotografier, informasjon om endringer av kryptosystemer, resultat av sikkerhetstester, detaljert nøkkelinformasjon og spesifikasjon av sikkerhetsstandarder for produksjon av kryptonøkler, og prosesser og metoder for å analysere kryptosystemer.

NSMs sertifiserte kryptoalgoritme skal merkes NSK.

Virksomhet som anskaffer kryptoutstyr kan overfor NSM foreslå klassifiseringen kontrollert kryptoutstyr (CCI) av spesifiserte ugraderte elektroniske eller akustiske komponenter eller utstyr, som tillates benyttet til håndtering av sikkerhetsgradert informasjon i informasjonssystemet. NSM avgjør klassifiseringen. Kontrollert kryptoutstyr tilsvarer NATOs betegnelse « Controlled Cryptographic Item » (CCI) og skal merkes CCI.

5.4 Til § 7-18 Distribusjon av kryptomateriell

NSM og virksomhet som leverer kryptosikkerhetstjenester skal påse at prosedyrer for sikker distribusjon, behandling, lagring, rapportering og regnskapsførsel er ivaretatt. Kryptomateriell fra NSM skal distribueres direkte til brukere eller til en underordnet kryptodistribusjonsmyndighet for videre distribusjon til brukere. Virksomhet som leverer kryptosikkerhetstjenester som er godkjent av NSM kan etablere tilsvarende distribusjonskanaler.

Følgende virksomheter leverer Kryptosikkerhetstjenester:

- NSM
- ERGO Group
- Kongsberg Defence Aerpspace (KDA)
- Thales Communications Noroway

Bestilling og avbestilling av kryptomateriell skal sendes tjenestevei til godkjenningsmyndigheten. NSM og virksomhet som leverer kryptosikkerhetstjenester fordeler materiellet etter oppdrag fra godkjenningsmyndigheten. Kryptonøkler til opplæring og testing skal bestilles direkte fra NSM eller virksomhet som leverer kryptosikkerhetstjenesten. Kryptonøklene skal ikke brukes til andre formål enn opplæring og testing.

Nasjonale kryptonøkler skal bestilles minst tre måneder før de skal tas i bruk. NATOs kryptonøkler skal bestilles minst seks måneder før de skal tas i bruk.

Alt krypto nøkkelmateriell skal produseres og distribueres i henhold til operativt behov fastsatt av overordnet operativ myndighet.

I denne forbindelse er overordnet operativ myndighet:

- Fellesoperativt hovedkvarter (FOHK)
- Utenriksdepartementet (UD)
- Politiets sikkerhetstjeneste (PST)
- Direktoratet for sivilt beredskap (DSB)
- Etteretningstjenesten

Godkjenningsmyndighet for nøkkelmateriell for testing, forsøk og prøvedrift i prosjekt kun for ugradert funksjonstesting er:

- Prosjektansvarlig
- Forvaltningen
- Kompetansesenter
- Involvert industri for testformål

Når behov for nøkkelmateriell er godkjent sender godkjenningsmyndigheten bestillingen til NSM som iverksetter nasjonal produksjon og/eller distribusjon. Dersom bestillingen gjelder NATO-materiell sender NSM bestillingen til NATO for produksjon og/eller distribusjon i henhold til NATOs prosedyrer for slike bestillinger.

Kryptomateriell inn og ut av Norge skal normalt gå gjennom NSM.

Tidsfrister ved bestilling av kryptomateriell
NATO nøkkelmateriell skal bestilles minimum 6 måneder og nasjonalt materiell 3 måneder før det skal tas i bruk.

NSM kan ikke garantere for levering av nøkkelmateriell, som ikke er bestilt i samsvar med ovennevnte frister.

Skjema for bestilling/avbestilling av kryptonøkkelmateriell er gitt i vedlegg.

Virksomheter med EKNAS/NOR skal benytte systemet til bestilling av alle typer kryptomateriell.

5.5 Til § 7-19 Forsendelse

Materiell merket KRYPTO skal sendes med kurer.

Ved forsendelse til utlandet av materiell merket NSK eller CCI skal kurer benyttes. I andre tilfeller kan materiell merket NSK eller CCI også sendes med registrert postsending eller andre metoder godkjent av NSM. Benyttes andre forsendelsesmetoder enn kurer skal avsender varsle mottaker om forsendelsesmetode og når forsendelsen kan ventes mottatt. Mottaker skal underrette avsender hvis forsendelsen ikke mottas til avtalt tid eller det er grunn til å tro at forsendelsen kan ha vært utenfor kontroll.

Elektronisk overføring av kryptonøkler skal skje i system godkjent av NSM.

Sikkerhetsgradert kryptomateriell skal ved forsendelse emballeres i samsvar med § 4-20, med de unntak og tillegg som følger av femte og sjette ledd i paragrafen her.

Ved forsendelse skal materiell merket KRYPTO sendes i dobbel emballasje. Materiell merket NSK eller CCI skal emballeres som for dokumenter gradert KONFIDENSIELT. For materiell merket KRYPTO, NSK eller CCI skal adressering og merking påføres emballasjen som for dokumenter gradert KONFIDENSIELT. I tillegg skal indre emballasje merkes « ÅPNES AV KRYPTOFORVALTER » eller navn på utpekt person. Eventuelt overføringsnummer skal påføres indre og ytre emballasje.

Ved forsendelse av kryptomateriell som ikke er merket KRYPTO, NSK eller CCI skal indre emballasje merkes « ÅPNES AV KRYPTOFORVALTER ». Overføringsnummer skal påføres indre og ytre emballasje. Ytre emballasje skal merkes med forsendelsesmetoden som anvendes, f.eks. « MED KURER » eller « REKOMMANDERT POSTSENDING ».

KRYPTO/CCI- materiell skal til enhver tid være under kontroll av nasjonale myndigheter. Forsendelse av denne typen materiell til utlandet, skal derfor gå fra nasjonal distribusjonsmyndighet (NDA) i Norge til NDA i mottakerlandet.

For nærmere beskrivelse av forsendelsesrutiner se vedlegg.

6 E. Kryptoregnskap

6.1 Til § 7-20 Etablering av kryptoregnskap

Enhver virksomhet som mottar kryptomateriell skal føre kryptoregnskap. Før kryptoregnskap etableres skal virksomheten sende en skriftlig anmodning om dette til NSM, underordnet kryptodistribusjonsmyndighet eller leverandør av kryptosikkerhetstjenester, som skal inneholde

1. *navn (tittel) og fullstendig adresse på virksomheten som anmoder om kryptoregnskap,*
2. *arten av kryptomateriell som skal installeres og tidspunktet virksomheten ønsker det i operativ drift,*
3. *bakgrunn og begrunnelse for å etablere kryptoregnskap,*

4. *beskrivelse og stadfesting av at minimumskravene til fysisk sikring for oppbevaring av kryptomateriell kan oppfylles,*

5. *navn og grad/stilling med fødselsnummer til personer som utpekes til kryptosikkerhetsleder, kryptoforvalter eller deres stedfortredere, og*

6. *signaturprøver til kryptoforvalter og dennes stedfortreder, undertegnet av virksomhetens leder.*

Anmodning om etablering av kryptoregnskap fra virksomheter i Forsvaret skal sendes gjennom overordnet operativ myndighet (FOHK) til NSM. Etteretningstjenesten anses i denne sammenhengen som selvstendig overordnet operativ myndighet.

Tilsvarende overordnet operativ myndighet ved sivile etater er UD, PST og DSB.

Forutsatt at de er godkjent av NSM er andre leverandører av kryptosikkerhetstjenester å betrakte som overordnet operativ myndighet for de virksomheter de leverer sikkerhetstjenester til.

Ved mottak av anmodningen kan NSM, underordnet kryptodistribusjonsmyndighet eller leverandør av kryptosikkerhetstjenester, etablere regnskapet og registrere åpningen av regnskapet og utpekingen av kryptoforvalter og dennes stedfortreder. Bekreftelse som stadfester etableringen av kryptoregnskapet skal sendes anmodende virksomhet.

6.2 Til § 7-21 Føring av kryptoregnskap

Kryptoregnskapet skal til enhver tid vise beholdningen av kryptomateriell.

Forslag til skjema for føring av kryptoregnskap er vist i vedlegg.

Om virksomheten har en omfattende kryptobeholdning, kan det være fornuftig å lage et elektronisk regnskap (database) i eksempelvis Excel eller Access. Om elektronisk regnskap benyttes må den datamaskinen som benyttes sikkerhetsmessig godkjennes for KONFIDENSIELT.

Lokal sjef kan sikkerhetsmessig godkjenne dedikert informasjonssystem opp til og med HEMMELIG, ref Forskrift om informasjonssikkerhet § 5-16.

Ved mottak av registrert kryptomateriell skal regnskapet uten opphold føres med angivelse av tittel, utgave, regnskapskode, antall og eventuelt registreringsnummer.

Dersom kryptomateriellet ikke har registreringsnummer og heller ikke behøver regnskapsføres med registreringsnummer, skal materiellet føres på regnskapsrapporten som ikke nummerert materiell med angivelsen « NN ».

Ved overføring eller tilintetgjøring av registrert kryptomateriell skal materiellet føres ut av regnskapet og rapport sendes distribusjonsmyndigheten.

6.3 Til § 7-22. Regnskapskoder

I kryptoregnskapet skal det benyttes følgende regnskapskoder (RK) utgitt av NSM, som tilsvarer NATOs Account Legend Codes (ALC), med tilhørende plikter vedrørende regnskapsføring og rapportering:

1. *RK 1: Materiellet skal regnskapsføres i alle distribusjonsledd med antall og registreringsnummer. Materiellet skal rapporteres.*

2. *RK 2: Materiellet skal regnskapsføres i alle distribusjonsledd med antall. Materiellet skal rapporteres.*

3. *RK 3: Materiellet skal regnskapsføres i alle distribusjonsledd med antall og registreringsnummer. Materiellet skal ikke rapporteres.*

4. *RK 4: Materiellet skal regnskapsføres i alle distribusjonsledd med antall. Materiellet kan i tillegg føres i det ordinære materiellregnskapet. Materiellet skal ikke rapporteres.*

5. *RK 5: Ikke i bruk.*

6. *RK 6: Elektroniske kryptonøkler skal regnskapsføres i alle distribusjonsledd med antall og registreringsnummer. Materiellet skal rapporteres.*

7. *RK 7: Elektroniske kryptonøkler som er lokalt distribuert skal regnskapsføres lokalt. Materiellet skal ikke rapporteres.*

NSM bestemmer i samråd med hovedforvalter hvilke regnskapskoder som skal benyttes for det enkelte materiell.

NSM kan dispensere fra bestemmelsene om regnskapsføring og rapportering.

6.4 Til § 7-23. Mottak og utlån av kryptomateriell

Ved mottak av kryptomateriell skal kryptoforvalter kontrollere at det er sendt på godkjent måte, at det ikke er brekkasje på ytre og indre emballasje og at innholdet stemmer med overføringsrapporten. Kryptoforvalter skal kvittere på originalen som skal returneres til avsender. Kvittert kopi skal oppbevares som bilag til lokalt regnskap i fem år. Kvittering kan skje elektronisk ved metode godkjent av NSM.

Ved utlån av kryptomateriell fra kryptoforvalter til andre innen virksomheten skal utlånskvittering benyttes. Brukere skal gjøres kjent med deres sikkerhetsmessige ansvar for materiellet inntil det er returnert til kryptoforvalter. Hvis brukere skal tilintetgjøre materiell skal de gjøres oppmerksom på bestemmelsene om tilintetgjøring i § 7-29 til § 7-34.

6.5 Til § 7-24 Mangfoldiggjøring

Mangfoldiggjøring av kryptonøkler og informasjon om sikkerhet ved kryptotjenesten er bare tillatt dersom utsteder har angitt dette eller NSM samtykker. Utdrag og kopier skal gis samme sikkerhetsgrad som originalen.

Dersom utsteder i forord eller på annen måte har tillatt mangfoldiggjøring, skal kopiene eller utdragene administreres etter de samme rutiner som originaldokumentet.

Der dette ikke er beskrevet bestemmer NSM reglene for mangfoldiggjøring.

NSM bestemmer om tillatelsen gis permanent, midlertidig eller for enkelttilfelle.

Disse retningslinjene gjelder uavhengig av om mangfoldiggjøringen foregår på papir eller elektroniske lagringsmedia

Utdrag og kopier skal regnskapsføres lokalt inntil de er tilintetgjort og skal påføres et identifikasjonsnummer.

Alle regnskapsbilag, kvitteringer, beholdnings- og tilintetgjøringsrapporter skal oppbevares i fem år og være tilgjengelig for innsyn.

Jf Forskriftens § 7-23 første ledd om mottak og utlån av kryptomateriell og § 7-25 rapportering.

Utdrag av kryptonøkler skal ikke beholdes lenger enn nødvendig og under enhver omstendighet ikke lenger enn 12 timer etter endt kryptoperiode.

6.6 Til § 7-25 Rapportering

Ved regnskap over kryptomateriell skal det benyttes

1. *overføringsrapport ved overføring av kryptomateriell fra ett kryptoregnskap til et annet,*
2. *mottaksrapport ved mottak av kryptomateriell der overføringsrapport mangler,*
3. *beholdningsrapport ved opptelling av fysisk beholdning av kryptomateriell, og*
4. *tilintetgjøringsrapport ved fysisk tilintetgjøring av kryptomateriell.*

Se vedlegg angående formatet til rapportene, overføringsrapport, mottaksrapport, beholdningsrapport og tilintetgjøringsrapport.

KNM og KV fartøyer skal sende beholdningsoppgave krypto til Sjøforsvarets Bokopplag innen den 15. i hver måned. Øvrige virksomheter skal sende beholdningsoppgave krypto to ganger i året, innen 15. april/15. oktober. Virksomheter som rapporterer direkte til NSM skal sende beholdningsoppgave innen 15. jun/15. des. Samtlige virksomheter skal sende makuleringsrapport krypto innen den 15. i hver måned. Virksomheter i utlandet eller andre som ikke har mulighet for å sende rapporter på fastlagt skjema, kan bruke elektronisk meldingstjeneste (sikkerhetsgodkjent for K O N F I D E N S I E L T). Rapporten sammen med meldingen skal oppbevares i lokalt kryptoregnskap.

Alt krypto/CCI-materiell med regnskapskode (RK) 1og 2 skal regnskapsføres i sentralt og lokalt kryptoregnskap. Det innebærer at holdere som mottar CCI-materiell fra NSM og senere overfører dette materiellet til andre regnskapssystemer plikter å telle opp materiellet i følge med innsendelse av beholdningsoppgave krypto.

Ved kontroll av beholdningsoppgave fra overordnet distribusjonsmyndighet kan det forekomme avvik.

Ved innsendelse av beholdningsoppgave skal alle avvik dokumenteres med bilag.

Rettelser i tilsendt beholdningsoppgave skal foretas med en enkel overstrykning og referanse til bilag.

Ved mottak av materiell skal kvitterte overføringspapirer returneres til utsteder uten ubegrunnet opphold, og senest innen 48 timer.

Er ikke rapporter eller overføringspapirer mottatt innen 30 dager, skal disse etterlyses, se vedlegg.

Underordnet kryptodistribusjonsmyndighet skal kontrollere rapporter fra virksomhetene og sende beholdningsrapport til NSM eller leverandør av kryptosikkerhetstjenester. Virksomheter som mottar kryptomateriell direkte fra NSM skal kontrollere beholdningen og sende beholdningsrapport til NSM.

Ved feil eller mangelfull rapportering skal den aktuelle distribusjonsmyndighet be om tilleggsrapport og iverksette andre nødvendige tiltak for å rette på forholdet.

Rapportering skal skje på fastlagt blankett eller elektronisk format godkjent av NSM.

I EKNAS/NOR er rapporteringsformatene tilgjengelig for bruker i brukergrensesnittet til systemet.

6.7 Til § 7-26 Sikkerhetsgradering av regnskap og rapporter

Kryptoregnskap og beholdningsrapporter med oppgave over kryptonøkler skal graderes KONFIDENSIELT. NSM bestemmer for det enkelte tilfelle sikkerhetsgrad for informasjon om kryptonøklers gyldighetsperiode.

Dersom rapportene påføres merknader eller annen informasjon som er gradert høyere en rapportens normale gradering, må rapporten påføres den høyeste graderingen. Makuleringsrapporter skal være gradert K O N F I D E N S I E L T uavhengig av antall poster.

I EKNAS/NOR skal rapportene ikke inneholde informasjon med høyere gradering enn K O N F I D E N S I E L T.

For øvrig skal regnskap og rapporter sikkerhetsgraderes etter sitt innhold, likevel minst BEGRENSET.

6.8 Til § 7-27. Kontroll av beholdning

Materiell klassifisert som RK 1, RK 2 eller RK 6 i samsvar med § 7-22, skal kontrolleres og rapporteres om minst hver sjette måned. Beholdningsrapport skal utarbeides på grunnlag av kryptoregnskapet. Den fysiske tilstedeværelsen av materiellet skal kontrolleres mot beholdningsoppgaven.

Kontrollen skal utføres av kryptoforvalter sammen med et kryptoautorisert vitne. Dersom et kryptoautorisert vitne ikke er tilgjengelig, kan et vitne sikkerhetsklarert for HEMMELIG delta i kontrollen, men skal ikke gis tilgang til kryptonøkler i klartekst. Kryptoforvalteren og vitnet skal signere beholdningsrapporten. Rapporten sendes til distribusjonsmyndigheten. Kopi av rapporten skal inngå som bilag til lokalt kryptoregnskap og skal bevares i fem år.

Dersom en virksomhet flyttes skal kryptomateriellet kontrolleres mot kryptoregnskapet og beholdningsoppgaven før pakking. Etter ankomst til ny lokalisering skal innholdet kontrolleres mot beholdningsoppgaven.

6.9 Til § 7-28 Avslutning av kryptoregnskap

Opphører behovet for kryptoregnskap, skal virksomheten sende anmodning til distribusjonsmyndigheten om at regnskapet avsluttes og om at ordningen med kryptosikkerhetsleder og kryptoforvalter med stedfortredere opphører.

Kryptoforvalter og stedfortredende kryptoforvalter skal utføre fysisk opptelling av alt registrert kryptomateriell og sende beholdningsoppgave til den aktuelle distribusjonsmyndighet. Distribusjonsmyndigheten skal gi instruksjoner om overføring av materiellet. Foreligger det mangler ved kryptoregnskapet skal samme prosedyrer følges som ved sikkerhetstruende hendelser.

Når gjøremål fastsatt i første og andre ledd er utført skal kryptoregnskapet overføres til den aktuelle distribusjonsmyndighet.

Ved avslutning av kryptoregnskap vil overordnet myndighet avgjøre hvilket kryptomateriell som skal makuleres eller innleveres til distribusjonsmyndigheten.

Det er meget viktig at avslutning av kryptoregnskapet blir utført i samsvar med § 7-28

for å sikre sporbarheten til materiellet.

7 F. Tilintetgjøring.

7.1 Til § 7-29 Tilintetgjøring av kryptonøkler

Kryptonøkler som har vært i bruk skal tilintetgjøres innen 12 timer etter endt gyldighetsperiode. Går gyldighetsperioden ut på en lørdag, søndag eller helligdag, skal tilintetgjøringen utføres første påfølgende virkedag. For kryptonøkler som består av flere segmenter med samme gyldighetsperiode skal det enkelte segment tilintetgjøres når det er lastet korrekt inn. Siste segment skal likevel beholdes i hele gyldighetsperioden.

For kryptonøkler som består av flere segmenter med samme gyldighetsperiode skal det enkelte segment tilintetgjøres når det er korrekt lastet inn. Siste segment for gyldighetsperioden skal beholdes og oppbevares i forseglet konvolutt. Segmentet skal pakkes inn i ugjennomsiktig materiale for eksempel sølv- eller blåpapir. Segmentet skal makuleres etter gyldighetsperiodens utløp. Konvolutten oppbevares som for annet nøkkelmateriell. I godkjente elektroniske lagringsenheter, der nøkkelen lagres kryptert, kan nøkkelsegmentet lagres i hele sin gyldighetsperiode.

Vedlegg er et eksempel på en segmentliste.

Fullstendige utgaver som ikke har vært i bruk skal tilintetgjøres innen fem dager etter endt gyldighetsperiode.

Testnøkler og nøkler for undervisningsformål som ikke er merket KRYPTO skal tilintetgjøres når de ikke lenger skal brukes.

Ukryptert kryptonøkkel som er lastet inn i nøkkellader for overføring, lagring eller innlasting av kryptonøkler, skal beskyttes i samsvar med sikkerhetsgraden på kryptonøkkelen. Kryptonøkkelen skal tilintetgjøres innen 12 timer etter innlasting.

Kryptert kryptonøkkel som er lastet inn i nøkkellader kan ligge i nøkkelladeren i hele gyldighetsperioden, men skal tilintetgjøres innen 12 timer etter endt gyldighetsperiode.

7.2 Til § 7-30. Tilintetgjøring av kryptodokumenter

Kryptodokumenter som er arkivverdige i henhold til arkivloven med forskrifter skal tilintetgjøres i samsvar med § 4-31.

Kryptodokumenter som ikke er arkivverdige skal tilintetgjøres innen 15 dager etter endt gyldighetsperiode.

7.3 Til § 7-31. Krav til personell som forestår tilintetgjøring

Tilintetgjøring av kryptonøkler skal foretas av kryptoforvalter sammen med et kryptoautorisert vitne, normalt stedfortredende kryptoforvalter. Dersom et kryptoautorisert vitne ikke er tilgjengelig kan isteden et vitne sikkerhetsklarert for HEMMELIG delta i tilintetgjøringen. Dersom kryptoforvalter eller dennes stedfortreder ikke er tilgjengelig innen fristen for tilintetgjøring, skal annet kryptoautorisert personell foreta tilintetgjøringen sammen med et vitne.

Ved mindre virksomheter hvor det i perioder bare er én kryptoautorisert person til stede, skal tilintetgjøring av kryptonøkler likevel utføres innen gjeldende frister. Årsaken til at bare én person har utført tilintetgjøringen skal anmerkes i listen for tilintetgjøring.

7.4 Til § 7-32. Metoder for tilintetgjøring

Tilintetgjøring av maskinell enhet av kryptoutstyr og nøkkelladere skal utføres i samsvar med brukerinstruks gitt for det enkelte utstyr.

Kryptonøkler og informasjon om sikkerheten ved kryptotjenesten skal uansett tilintetgjøres som for STRENGT HEMMELIG i § 4-36.

Tilintetgjøring av annet kryptomateriell skal utføres i samsvar med metode i § 4-36 for materiellets sikkerhetsgrad.

7.5 Til § 7-33 Tilintetgjøringsrapport

Ved tilintetgjøring av kryptomateriell skal det utferdiges tilintetgjøringsrapport. Tilintetgjøringsrapporten skal inneholde et løpenummer, kryptomateriellets tittel, utgave, antall og registreringsnummer. Rapporter på papir skal være påført teksten « Siste post » etter siste linje.

I vedlegg er det gitt eksempel på tilintetgjøringsrapport.

Etter tilintetgjøringen skal rapporten signeres av det personellet som har utført tilintetgjøringen og graderes KONFIDENSIELT.

Tilintetgjøringsrapporten skal sendes distribusjonsmyndigheten. Kopi av rapporten skal bevares som bilag i lokalt kryptoregnskap i fem år.

Ved tilintetgjøring av segmenter av kryptonøkler skal segmentlisten signeres av det personellet som har utført tilintetgjøringen. Segmentlisten skal oppbevares som bilag i lokalt kryptoregnskap i fem år.

I vedlegg er det gitt eksempel på segmentliste.

7.6 Til § 7-34. Evakuering og ekstraordinær tilintetgjøring

For evakuering og ekstraordinær tilintetgjøring av kryptomateriell gjelder bestemmelsene i § 4-35, med følgende unntak og tillegg:

1. *Kravet om samling i lett transportable beholdere gjelder bare for kryptonøkler og kryptodokumenter.*

2. *Får virksomheten etter en evakuering igjen kontroll over området skal det foretas opptelling av alt kryptomateriell. Ved mangler skal rapportering skje i samsvar med § 7-41 og § 7-45.*

3. *Ved ekstraordinær tilintetgjøring skal kryptonøkler tilintetgjøres først i følgende rekkefølge; nøkler med utgått gyldighetsperiode, gyldige nøkler og reservenøkler. Deretter skal kryptoutstyr merket KRYPTO, NSK eller CCI tilintetgjøres. Til slutt skal annet kryptomateriell tilintetgjøres. Tilintetgjøringsrapport skal om mulig sendes distribusjonsmyndigheten.*

8 G. Fysisk sikring.

8.1 Til § 7- 35 Sikring av kryptomateriell

Kryptoutstyr som det stilles krav om kryptoautorisasjon for å bruke skal installeres i kryptorom. Det skal i tillegg opprettes sperret område.

Bestemmelser for beskyttelse av NATO-gradert informasjon som er beskrevet i C-M 2002 - 49 gjelder også for kryptomateriell.

Kryptoutstyr som det ikke stilles krav om kryptoautorisasjon for å bruke kan installeres i kontrollert område, kontorer eller private hjem, dersom det er beskyttet med manipulasjonssikring godkjent av NSM. Kravene til fysisk sikring fremgår av brukerinstruksen til det enkelte utstyr.

Kryptoutstyr med kryptonøkkel som tillates oppbevart i personlig varetekt skal være under personlig kontroll, nedlåst eller avlåst på godkjent måte, i samsvar med brukerinstruks for det enkelte type utstyr.

Kryptoutstyr merket NSK eller CCI og som ikke er i bruk skal lagres tilsvarende som informasjon gradert KONFIDENSIELT.

Se nærmere bestemmelser for behandling av CCI materiell

8.2 Til § 7-36. Sikring av kryptorom

Ved nybygg og ombygging av kryptorom skal det ikke fremgå av ugraderte tegninger eller lignende hva rommet skal nyttes til.

Mobile enheter kan benyttes som kryptorom dersom disse er godkjent av NSM.

Kryptorom skal sikres tilsvarende som sperret område med informasjon gradert KONFIDENSIELT. Rommet skal plasseres slik i bygningen at det oppnås størst mulig avstand til områder hvor det ikke utøves fysisk kontroll, og slik at tilstøtende rom og arealer kan kontrolleres og sikres. Plasseringen av kryptorom skal være godkjent av NSM.

Dersom det ikke er mulig å stillet eget rom til disposisjon kan kryptotjenesten foregå i et rom som også blir benyttet til andre formål. Personell uten kryptoautorisasjon skal i så fall ikke ha adgang til rommet når kryptotjeneste utøves. Ordningen skal være godkjent av NSM.

Dører til kryptorom skal være av minimum 40 millimeter heltre eller tilsvarende styrkenivå og være forsvarlig montert. Dersom døren er utvendig hengslet, skal den sikres i bakkant.

Veggene skal gå fra gulv til fast tak og skal ikke kunne demonteres fra utsiden uten at det avsettes spor. I rom med nedsenket himling skal område mellom himling og tak være kontrollerbart.

Kryptorom skal om mulig ikke ha vinduer. Har rommet likevel vinduer skal vinduene være skjermet slik at de ikke slipper gjennom lys og sikret slik at det ikke er mulig å trenge inn i rommet uten å avsette spor.

Ventiler, kanaler og tilsvarende åpninger skal sikres mot inntrenging. Åpninger som er mindre enn 600 cm^2 skal ha installert lydfeller. Åpninger som er større enn 600 cm^2 skal i tillegg ha installert gitter eller overvåkingssystem som beskrevet i § 6-9 syvende ledd andre til fjerde punktum.

Helautomatiske ubemannede kryptorom skal sikres med spesielle tiltak etter anvisning fra NSM i hvert enkelt tilfelle.

8.3 Til § 7-37 Adgangskontroll

Det skal gjennomføres kontroll med adgangen til kryptorom. For adgang kreves kryptoautorisasjon. Det skal foreligge en liste over personell som har permanent adgang. Listen skal signeres av virksomhetens leder. Bare én dør skal benyttes for inn- og utpassering. Andre dører skal være forsvarlig sikret mot inntrenging

og skal bare kunne åpnes fra innsiden. Besøkende med tjenstlig behov kan få adgang dersom det er godkjent av virksomhetens leder og de ledsages av personell med permanent adgang. Besøkende skal legitimere seg og registreres i protokoll eller lignende besøksregister. Besøksregisteret skal bevares i minst ti år.

Vedlegg viser et skjema for besøkslogg. Besøksloggen skal oppbevares i 10 år.

I områder hvor det oppbevares store mengder kryptonøkler eller hvor det kryptonøkler produseres eller administreres, skal det etableres adgangsrutiner som sikrer at det alltid er to kryptoautoriserte personer til stede samtidig.

8.4 Til § 7-38. Oppbevaring

Kryptomateriell merket KRYPTO skal oppbevares som for informasjon gradert HEMMELIG.

Kryptonøkler merket NSK og gradert BEGRENSET skal oppbevares som for informasjon gradert HEMMELIG. Slike kryptonøkler kan likevel oppbevares som for KONFIDENSIELT dersom virksomheten ikke har oppbevaringsenhet for HEMMELIG.

Dersom personell uten kryptoautorisasjon skal ha tilgang til oppbevaringsenhet som inneholder materiell merket KRYPTO, skal personellet ha sikkerhetsklarering for minst HEMMELIG/tilsvarende og materiellet skal oppbevares i indre låsbar enhet som bare kryptoautorisert personell kan åpne.

Reservekryptonøkler skal oppbevares adskilt fra gyldige kryptonøkler.

8.5 Til § 7-39 Låser og nøkler.

Låsenheter som sikrer oppbevaringsenheter og rom med kryptomateriell skal være godkjent av NSM. Låsene skal ikke inngå i sentralt låssystem. Tap eller kompromittering av låser, nøkler eller kombinasjoner skal straks meldes til kryptosikkerhetsleder og virksomhetens leder.

Nøkler for adgang til kryptorom skal oppbevares som for KONFIDENSIELT, og bare være tilgjengelig for kryptoautorisert personell.

Nøkler og kombinasjoner til oppbevaringsenheter for kryptomateriell, skal oppbevares i samsvar med kravene til oppbevaring av det materiellet de beskytter.

Nøkler skal opptelles minst hver sjette måned. Dato og signatur fra den som utfører opptellingen skal påføres kontrollskjema, kvittering eller lignende.

I vedlegg er vist kontrollskjema (nøkkelinstruks) for behandling og kontroll av nøkler.

8.6 Til § 7-40 Installasjon av kryptoutstyr

Kryptoutstyr skal beskyttes i samsvar med § 5-6 og vedlegg 1 og installasjonen skal godkjennes av NSM. Etter at installasjonen er godkjent skal det ikke gjøres noen endringer, med mindre det innhentes ny godkjenning.

Kryptoutstyr og kryptosystemer blir vanligvis utplassert av hovedforvalter eller den NSM bemyndiger. Godkjenningsmyndighet er i utgangspunktet NSM for alle kryptoinstallasjoner. Nærmere bestemmelser vil bli gitt.

Installatøren skal forsikre seg om at nødvendig kryptoorganisasjon og instruksverk er på plass. På bakgrunn av informasjon fra installatøren kan godkjenningsmyndigheten gi midlertidig godkjenning.

Endelig godkjenning vil bli gitt etter at godkjenningsmyndigheten har vært på befaring.

9 H. Reaksjon ved sikkerhetstruende hendelser.

9.1 Til § 7-41. Typer sikkerhetstruende hendelser

Operative og tekniske sikkerhetstruende hendelser i form av funksjonsfeil og produksjonsfeil på kryptoutstyr, og operatørfeil som har innvirkning på kryptosikkerheten, omfatter blant annet

1. *bruk av kryptonøkkel som enten er kompromittert, tidligere brukt og ikke godkjent for gjenbruk, brukt til andre formål enn den er godkjent for, brukt utenfor den tidsperiode den er godkjent for, eller som ikke er godkjent av NSM,*
2. *avvik fra vedlikeholdsinstruks for et spesifikt kryptoutstyr,*
3. *utført eller forsøk på reparasjon eller vedlikehold foretatt av uautorisert personell,*
4. *bruk av forbindelse som ikke er kryptert for å omtale detaljer om feil og feilfunksjoner på kryptoutstyr,*
5. *forsøk på eller utført modifisering av kryptoutstyr uten godkjennelse, og*
6. *kompromitterende elektromagnetisk stråling (tempest) fra kryptoutstyr.*

Personellmessige sikkerhetstruende hendelser i form av at personer med adgang til kryptomateriell kan ha innvirkning på sikkerheten til kryptomateriell, omfatter blant annet tilfeller der det kan være grunn til å revurdere en persons sikkerhetsklarering og tilfeller hvor det har foregått eller vært forsøk på ulovlig utlevering av informasjon om kryptomateriell.

Fysiske sikkerhetstruende hendelser i form av tap, tyveri, manipulering, uautorisert adgang eller innsyn vedrørende kryptomateriell, eller forsøk på slike handlinger, omfatter blant annet

1. *kryptomateriell som er rapportert tilintetgjort, men hvor tilintetgjøring ikke har funnet sted,*
2. *kryptomateriell som ikke er fullstendig tilintetgjort og deretter forlatt uten tilsyn,*
3. *forsendelse av kryptomateriell utenfor godkjent distribusjonskanal,*
4. *kryptomateriell som ikke er korrekt pakket, mottatt med skadet emballasje, eller uforklarlig brekkasje av forsegling på kryptonøkler,*
5. *bruk av tilintetgjøringsmetoder som ikke er godkjent,*

6. *mangfoldiggjøring eller reproduksjon av kryptonøkler som ikke er godkjent av NSM eller andre virksomheter som produserer kryptonøkler,*

7. *brudd på eventuelle krav om tilstedeværelse av to personer samtidig for behandling av kryptomateriell,*

8. *forfalskning av kryptodokumenter eller kryptonøkler, og*

9. *manipulering eller inntrenging i et kryptosystem, konstatering av elektroniske overvåkings- eller opptaksanordninger nær et kryptosystem, eller utløsning av sikkerhetsmekanismer mot manipulasjon.*

9.2 Til § 7-42. Generelt om rapporterings- og tiltaksplikt

Alt personell som har tilgang til kryptomateriell skal gjøres oppmerksom på nødvendigheten av straks å rapportere sikkerhetstruende hendelser til kryptosikkerhetsleder. Kryptosikkerhetsleder skal rapportere videre til virksomhetens leder. Virksomheten skal omgående rapportere videre og iverksette umiddelbare tiltak som kan redusere mulige skadevirkninger.

Rapporten skal sendes i det format og med de opplysninger som NSM fastsetter som standard eller for det enkelte tilfelle.

9.3 Til § 7-43 Nærmere om rapportering

Foreløpig rapport skal avgis ved sikkerhetstruende hendelser. Slik rapport skal avgis innen 24 timer dersom den omhandler kryptonøkler som er gyldige eller blir gyldige innen 15 dager, spionasje, manipulering eller sabotasje mot kryptomateriell, eller mangfoldiggjøring eller reproduksjon av kryptomateriell som ikke er godkjent av NSM. Rapport skal avgis innen 48 timer dersom den omhandler reservekryptonøkler som blir gyldige etter 15 dager eller kryptonøkler med utgått eller ikke angitt gyldighetsperiode, eller innen 72 timer dersom den omhandler andre sikkerhetstruende hendelser.

I vedlegg er det vist eksempel på foreløpig rapport.

Utfyllende rapport skal avgis når det fremkommer ny viktig informasjon om et tidligere rapportert forhold.

I vedlegg er det vist eksempel på utfyllende rapport.

Endelig rapport skal inneholde en sammenfatning av resultater om alle innhentede opplysninger og undersøkelser, og opplyse om tiltak som er gjennomført eller planlagt for å begrense muligheten for gjentakelse. Foreløpig rapport eller utfyllende rapport kan tjene som endelig rapport dersom den tilfredsstiller kravene til endelig rapport.

I vedlegg er det vist eksempel på endelig rapport.

Foreløpig, utfyllende og endelig rapport skal sikkerhetsgraderes etter sitt innhold, og om mulig sendes elektronisk med kommunikasjonsmiddel godkjent for aktuell sikkerhetsgrad. Dersom elektroniske kommunikasjonsmidler ikke er

tilgjengelig skal rapport om forhold som nevnt i § 7-41 første og andre ledd sendes i samsvar med § 7-19.

For NATO materiell skal rapporteringen følge retningslinjene i AMSG 293 chapter 10.

9.4 Til § 7-44 Adressater for rapportering av nasjonalt materiell

Rapporter som gjelder nasjonalt kryptomateriell skal sendes til NSM eller annen virksomhet som leverer kryptosikkerhetstjenester. Kopi av rapporten skal sendes til overordnet virksomhet og virksomheten hvor den sikkerhetstruende hendelsen fant sted.

Alle virksomheter med NSM som leverandør av kryptosikkerhetstjenester skal rapportere til overordnet myndighet og NSM.

Øvrige virksomheter skal rapportere til sin leverandør av kryptosikkerhetstjenester.

9.5 Til § 7-45 Adressater for rapportering av NATO materiell

Rapporter om forhold som nevnt i § 7-41 første og annet ledd vedrørende NATOs kryptomateriell skal sendes til den som er kontrollerende myndighet i henhold til NATOs publikasjon « AMSG 600 ». Ved forbindelse punkt til punkt er virksomhet som har kryptonøkkel med registreringsnummer 1 kontrollerende myndighet. Kopi av rapporten skal sendes til NATO Security and Evaluation Agency (SECAN), European Security and Evaluation Agency (EUSEC) og NSM.

Dersom rapporterende virksomhet ikke er kjent med hvem som er kontrollerende myndighet etter første ledd, skal rapport sendes til SECAN med kopi til EUSEC og NSM.

Dersom det er flere kontrollerende myndigheter for samme kryptomateriell, skal rapport sendes til SECAN og EUSEC med kopi til kontrollerende myndigheter og NSM.

Ved sikkerhetstruende hendelser hos kontrollerende myndighet skal rapport sendes til SECAN med kopi til EUSEC og NSM.

For rapporter om forhold som nevnt i § 7-41 tredje ledd vedrørende NATOs kryptomateriell, skal det for kryptomateriell hvor EUSEC er kontrollerende myndighet sendes rapport til EUSEC, med kopi til SECAN og NSM.

Rapportering skal følge retningslinjene i AMSG 293 Chapter 10.

Vedlegg A Dokumenthistorie

2002-10-13 Versjon 1

2007-04-19 Versjon 2