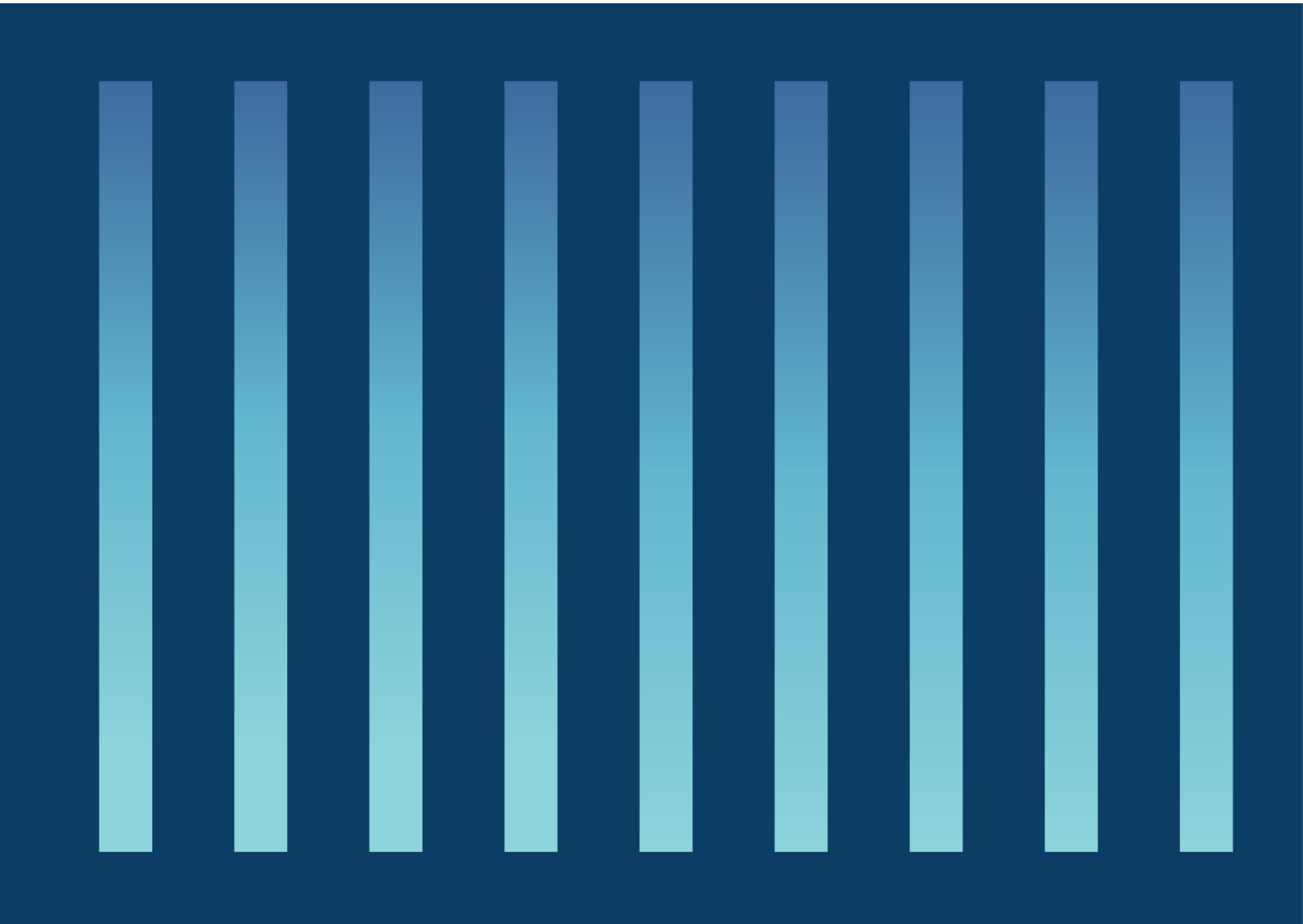
NASJONAL
SIKKERHETSMYNDIGHET

Veileder for godkjenning og implementering av kryptosystemer

versjon 2022-01-31; *G:21/971 rev. 2*



Nasjonal sikkerhetsmyndighet (NSM) er fagorgan for forebyggende sikkerhet, og sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven). NSM skal gi informasjon, råd og veiledning om forebyggende sikkerhetsarbeid.

Sikkerhetsloven med tilhørende forskrifter trådte i kraft 1. januar 2019. Loven skal bidra til å forebygge, avdekke og motvirke tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser.

Sikkerhetsloven gjelder for statlige, fylkeskommunale og kommunale organer og for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser. De enkelte departementer skal innenfor sitt ansvarsområde vedta at andre virksomheter skal underlegges loven dersom de behandler sikkerhetsgradert informasjon eller råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller driver aktivitet som har avgjørende betydning for disse funksjonene.

NSMs veiledninger utdyper regelverkforståelsen, herunder den tematiske sammenhengen mellom ulike bestemmelser i sikkerhetsloven og tilhørende forskrifter. Veilederne representerer NSMs syn på hvordan lov og forskrifter er å forstå, og danner et grunnlag for virksomhetenes arbeid med å etterleve regelverket.

NSM gir i tillegg ut håndbøker og tekniske råd som gir mer utfyllende anbefalinger om hvordan lovens funksjonelle krav kan oppfylles. Håndbøkene og de tekniske rådene beskriver fremgangsmåter, prosedyrer og gir eksempler på tiltak for å hjelpe virksomhetene i regelverksanvendelsen.

Veilederen anbefales lest i sammenheng med lov og forskrift, samt NSMs øvrige relevante veiledere, håndbøker og tekniske råd.

INNHOLD

1. Formål og omfang

Denne veilederen omhandler godkjenning av kryptosystemer som skal beskytte sikkerhetsgradert informasjon, og godkjenning av informasjonssystemer som implementerer kryptosystemer som sikkerhetstiltak. Veilederen omhandler ikke utvikling av kryptosystemer.

Målgruppen for denne veilederen er personell som har ansvar for IKT- eller kryptosikkerhet i en virksomhet som bruker eller skal bruke kryptosystem som sikkerhetstiltak, og personell med forvaltningsansvar for kryptosystemer eller skjermingsverdige informasjonssystemer.

Veilederens anbefalinger om beskyttelse av informasjon sikkerhetsgradert BEGRENSET er også anvendelige for skjermingsverdig informasjon som ikke er sikkerhetsgradert, der virksomheten likevel ser behov for å benytte kryptosystemer for å beskytte informasjon.

2. Bakgrunn og definisjoner

En trusselaktør som forserer et kryptosystem oppnår ikke-detekterbar adgang til passivt å overvåke informasjonssystemet som det beskytter. Sikkerhetsgradert informasjon kan ha behov for beskyttelse over flere tiår. Trusselaktører som ikke har kapasitet til å forsere et gitt kryptosystem, vil derfor kunne lagre krypterte data med en ambisjon om å etablere en forseringskapasitet på et senere tidspunkt, og dermed dekryptere de lagrede data.

Kryptosystemer må altså være motstandsdyktige mot sofistikerte trusselaktører med god tid og mye ressurser. Det er derfor nødvendig å ha en høy grad av tillit til produsenter av kryptosystemer, og til organisasjoner som gjør evaluering og sertifisering av dem, for igjen å kunne ha høy grad av tillit til kryptosystemenes korrekte virkemåte. Like viktig er det at kryptosystemer implementeres, brukes, driftes og forvaltes på en god måte i de organisasjoner og informasjonssystemer der de settes i drift.

Lov om nasjonal sikkerhet (heretter *sikkerhetsloven*) med forskrifter oppstiller plikter for virksomheter som skal bruke kryptosystemer for å beskytte sikkerhetsgradert informasjon, og gir oppgaver til sikkerhetsmyndigheten, dvs. Nasjonal sikkerhetsmyndighet (NSM), som godkjenningsmyndighet for kryptosystemer og overordnet nasjonal forvalter av kryptoutstyr.

Godkjenning av kryptosystemer bør ses fra et informasjonssystemperspektiv. Behovet for å bruke kryptosystemer utløses av et behov for å beskytte sikkerhetsgradert informasjon som behandles i et informasjonssystem. Det er flere typer godkjenninger som må på plass før en virksomhet kan etablere slike informasjonssystemer, og behovet for tillit til løsninger og omkringliggende prosesser varierer med informasjonens sikkerhetsgrad og den risiko som informasjonen er utsatt for.

Denne veilederen tar for seg veien fram til de nødvendige godkjenningsvedtak, herunder:

- NSMs godkjenning av kryptosystem, jf. sikkerhetsloven § 5-6, som skal beskytte sikkerhetsgradert informasjon.

- Godkjenningsmyndighetens godkjenning av informasjonssystem, jf. sikkerhetsloven § 6-3, som behandler sikkerhetsgradert informasjon og som benytter kryptosystem(er) som sikkerhetstiltak.
- Øvrige godkjenninger og krav til sikker drift av kryptosystemer som del av informasjonssystem, herunder til virksomhetens styringssystem for sikkerhet.

Veilederens kapittel 3 beskriver de overordnede prosessene. Kapittel 4 og 5 gir innsikt i NSMs vurderinger i forbindelse med godkjenning av hhv. kryptosystemer og informasjonssystemer som benytter kryptosystemer som sikkerhetstiltak. Organisatoriske og personellmessige tiltak inngår i kapittel 5. Kapittel 6 behandler øvrige godkjenningsplikter i forskrift om kryptosikkerhet.

Veilederen benytter følgende terminologi på følgende måte:

Kryptoutstyr:	Utstyr som, ved hjelp av kryptografiske mekanismer[1] og som hovedfunksjon, beskytter sikkerhetsgradert informasjons konfidensialitet, integritet, autentisitet eller tilgjengelighet. Kryptoutstyr inngår i et kryptosystem.
Kryptosystem:	Et system som på en helhetlig måte tilbyr sikkerhetstjenester relatert til konfidensialitet, integritet, autentisitet eller tilgjengelighet til et informasjonssystem som behandler sikkerhetsgradert informasjon, og som består av en eller flere samhandlende kryptografiske mekanismer, enten i kryptoutstyr eller i programvare i andre typer utstyr, samt tilhørende styrings- og konfigureringsløsninger.
Kryptonøkkel:	Særlig sensitiv informasjon benyttet av kryptosystemer som parameter til kryptografiske mekanismer, og som må aktivt og sikkert forvaltes for at et kryptosystem kan tilby sikkerhetstjenester.
Informasjonssystem[2]:	System som behandler—herunder transporterer, lagrer eller prosesserer—informasjon, og som anvendes for å løse en oppgave eller utføre en funksjon i en organisasjon. Det omfatter menneskelige, organisatoriske og tekniske ressurser, metoder og teknikker.

NSM skiller mellom kryptosystemer som kan beskytte informasjon sikkerhetsgradert høyst BEGRENSET (heretter *lavgradert informasjon*), og kryptosystemer spesielt utviklet for å beskytte informasjon sikkerhetsgradert KONFIDENSIELT og høyere (heretter *høygradert informasjon*).

Vi har andre og sterkere krav til tillit til kryptosystemer som kan beskytte høygradert informasjon enn til kryptosystemer som kan beskytte høyst lavgradert informasjon. Kryptosystemer som kan beskytte høyst lavgradert informasjon inkluderer rent kommersielle krypteringsløsninger tilgjengelig på det åpne

[1] Med *kryptografiske mekanismer* mener vi implementasjoner av kryptografiske algoritmer med hensikt å levere sikkerhetstjenester relatert til konfidensialitet, integritet, autentisitet eller tilgjengelighet. Begrepet inkluderer, men er ikke avgrenset til, kryptering og dekryptering, og generering og validering av digitale signaturer.

[2] Definisjonen er basert på begreper fra Prop. 153 L (2016-2017), *Lov om nasjonal sikkerhet (sikkerhetsloven)*, kapittel 19.6 (som omhandler merknader til proposisjonens lovforslags § 6-1).

marked. Kryptosystemer som kan beskytte høygradert informasjon er spesialutviklede kryptosystemer underlagt streng kontroll av produsentlandets sikkerhetsmyndigheter, og er vanligvis underlagt eksportkontroll jf. eksportkontrolloven.

I denne veilederen deler vi disse i to klasser som håndteres forskjellig; kryptosystemer som kan beskytte høyst lavgradert informasjon omtales heretter som *kommersielle kryptosystemer*[3], og kryptosystemer som kan beskytte høygradert informasjon omtales som *høytillitskryptosystemer*.

3. Prosesser

NSM bruker forskjellige prosesser for informasjonssystemer som skal benytte kommersielle kryptosystemer og de som skal benytte høytillitskryptosystemer.

For informasjonssystemer som skal benytte kommersielle kryptosystemer ses godkjenning av kryptosystemer etter § 5-6 konkret i sammenheng med informasjonssystemet som kryptosystemene skal beskytte og være en del av. Dette innebærer at godkjenning av kryptosystemene bør gjøres sammen med godkjenning av informasjonssystemet. For høytillitskryptosystemer, vil NSM utstede godkjenning av hvert kryptosystemet uavhengig av informasjonssystem.

De overordnede prosessene beskrives kort under. Kapittel 4 og 5 underbygger disse overordnede beskrivelsene.

Felles for prosessene er at de begynner med at behovet for å implementere et kryptosystem identifiseres:

F1. Virksomheten identifiserer, gjennom sitt arbeid med å håndtere risiko, et behov for å beskytte sikkerhetsgradert informasjon i et informasjonssystem ved hjelp av kryptoteknologi som ledd i utvikling av informasjonssystemet, eller som en del av det kontinuerlige arbeidet med å håndtere risiko.
F2. Virksomheten vurderer om kommersielt kryptosystem reduserer risiko tilstrekkelig til å etablere forsvarlig sikkerhetsnivå, eller om høytillitskryptosystem må benyttes.

Ofte vil det alene være sikkerhetsgraden til informasjonen som skal beskyttes som bestemmer om et kommersielt kryptosystem kan benyttes, eller om et høytillitskryptosystem må benyttes. Det kan likevel være tilfeller der en etter at en risikovurdering finner det nødvendig å bruke høytillitskryptosystemer for å etablere et forsvarlig sikkerhetsnivå også for informasjonssystemer som behandler lavgradert informasjon.

Den videre prosessen er avhengig av hvilken klasse kryptosystemer det er behov for.

[3] Begrepet er noe upresist, da det også dekker kryptosystemer som ikke er tilgjengelig på det åpne markedet, men som er implementert med tilsvarende grad av tillit som kommersielt tilgjengelige kryptosystemer.

For kommersielle kryptosystemer:

K1. Virksomheten velger kryptosystem på lik linje med andre sikkerhetstiltak. Ved valg av kryptosystem må virksomheten vurdere om det valgte systemet reduserer risiko tilstrekkelig slik at virksomheten kan etablere forsvarlig sikkerhetsnivå jf. virksomhetsikkerhetsforskriften § 49, med hensyn til §§ 16 og 17.
K2. Virksomheten beskriver kryptosystemets implementering, bruk, drift og forvaltning som del av beskrivelsen av informasjonssystemet jf. NSMs Veileder for godkjenning av informasjonssystem[4].
K3. Virksomheten søker godkjenningsmyndigheten om godkjenning av informasjonssystemet, jf. sikkerhetsloven § 6-3, der man også tilkjennegir at informasjonssystemet benytter kryptosystem godkjenningspliktig etter § 5-6.
K4. Godkjenningsmyndigheten, om dette er annen myndighet enn NSM og godkjenningsmyndigheten anser at valg av kryptosystem er hensiktsmessig, søker NSM om godkjenning av kryptosystemet slik det implementeres, brukes, driftes og forvaltes som del av informasjonssystemet på vegne av virksomheten. Dersom godkjenningsmyndigheten er NSM, treffes vedtak etter sikkerhetsloven §§ 5-6 og 6-3 i samme saksgang.

For bruk av høytillitskryptosystemer vil prosessen være avhengig av om relevante produkter allerede er godkjent av NSM, og ført på NSMs liste over godkjente kryptosystemer. Prosessen for å få godkjent et informasjonssystem forutsetter altså at det foreligger et relevant og godkjent kryptosystem. Godkjente høytillitskryptosystem vil typisk være produkter tilgjengelig fra en leverandør[5]. Prosessen for godkjenning av slike produkter er som følger:

P1. Virksomheten vurderer egnede kryptosystemer. Virksomheten bør søke råd og veiledning hos NSM i dette arbeidet.
P2. Virksomheten søker NSM om godkjenning av det aktuelle kryptosystemet for bruk til å beskytte høygradert informasjon.
P3. NSM treffer vedtak etter sikkerhetsloven § 5-6. Ved positivt vedtak, føres kryptosystemet opp på NSMs liste over godkjente høytillitskryptosystemer. Oppføringen vil gi informasjon om produktets aksepterte bruksområde og krav til implementering, bruk, drift og forvaltning. Godkjenningen vil gjelde for alle norske virksomheter om ikke annet avtales med søker eller andre forhold tilsier at godkjenningen bør gjelde mer begrenset.

Prosessen for godkjenning av informasjonssystem som benytter godkjent høytillitskryptosystem kan da gjennomføres:

H1. Når et egnet kryptosystem finnes i NSMs liste over godkjente høytillitskryptosystemer, beskrives kryptosystemets implementering, bruk, drift og forvaltning innenfor rammen av krav fremsatt av NSM sammen med godkjenningen av kryptosystemet, som del av beskrivelsen av informasjonssystemet.

[4] Tilgjengelig på NSMs internettsider.

[5] Til forskjell fra kommersielle kryptosystemer som *kan* være sammensatt av forskjellige kommersielle produkter av den som utvikler et informasjonssystem. NSM anbefaler at også kommersielle kryptosystemer er evaluerte og sertifiserte produkter.

H2. Virksomheten søker godkjenningsmyndigheten om godkjenning av informasjonssystemet, jf. sikkerhetsloven § 6-3, der man tilkjennegir at informasjonssystemet benytter høytillitskryptosystem som er godkjent etter sikkerhetsloven § 5-6.

H3. Godkjenningsmyndigheten vurderer som ledd i sin saksbehandling om kryptosystemets implementering, bruk, drift og forvaltning er i samsvar med krav framsatt av NSM og for øvrig er i tråd med informasjonssystemets sikkerhetsmål.

Informasjonssystemer kan ha behov for å benytte både kommersielle kryptosystemer og høytillitskryptosystemer for å etablere et forsvarlig sikkerhetsnivå. Det vil i så fall være nødvendig å gjennomføre prosessene over i kombinasjon.

Prosessene som er beskrevet over er ment å være veiledende. Avvik kan forekomme i forbindelse med saksbehandling av den enkelte sak. Innholdet i prosessene beskrives nærmere i de følgende kapitlene.

4. Godkjenning av kryptosystem

Kryptosystemer benyttes som sikkerhetstiltak i informasjonssystemer, og ofte er kryptosystemet avgjørende for å sikre at personer ikke får tilgang til sikkerhetsgradert informasjon de ikke er autorisert for. Virksomhetsikkerhetsforskriften §§ 16 og 17 oppstiller krav til evaluering og sertifisering av slike produkter. NSMs godkjenning av kryptosystem hviler på, og validerer, et kryptosystems evaluering og sertifisering.

Ved godkjenning av kryptosystemer vurderer NSM om kryptosystemene implementerer hensiktsmessig kryptoteknologi[6] og om kryptoteknologien er implementert med en tilstrekkelig grad av tillit til korrekt virkemåte. Jo høyere sikkerhetsgrad informasjonen som skal beskyttes har, jo høyere krav til tillit må NSM stille til kryptosystemet.

Evaluerte og sertifiserte sikkerhetsprodukter, slik som kryptosystemer, må brukes iht. forutsetninger gitt underveis i utvikling, produksjon, evaluering og sertifisering. Slike forutsetninger kommer gjerne til uttrykk i brukermanualer og øvrig dokumentasjon fra produsent, og i instrukser fra sertifiserende myndighet. I forbindelse med godkjenning av et kryptosystem kan NSM stille krav til implementering, bruk, drift og forvaltning. Virksomheter som bruker slike kryptosystemer er forpliktet til å følge disse kravene, jf. virksomhetsikkerhetsforskriften § 27, fjerde ledd.

[6] Jf. NSM Cryptographic Recommendations, tilgjengelig på NSMs internettsider.

4.1. Særskilt for høytillitskryptosystemer

Det er en forutsetning at høytillitskryptosystemer som er tenkt brukt av norske virksomheter er evaluert og sertifisert av produsentnasjonen. I dette ligger det en forventning om at kryptosystemet er tatt fram under produsentnasjonens sikkerhetsmyndigheters direkte kontroll og at disse har etablert tilstrekkelig tillit til at kryptosystemet kan beskytte nasjonens egen høygraderte informasjon. Dette gjelder også for norskproduserte kryptosystemer, og utvikling av kryptosystemer skal reguleres i en avtale mellom NSM og kryptoprodusenten.

For å kunne godkjenne et kryptosystem må NSM etablere tillit til produsentnasjonen generelt, og mer spesifikt til produsentnasjonens kryptoutstyrsprodusent, sikkerhetsevaluering og sertifiseringsprosess. Avhengig av hvilken grad av tillit Norge og NSM har eller oppnår til produsentnasjonen, vil det kunne være nødvendig å kreve en nasjonal evaluering av det utenlandske kryptosystemet før en kan si å ha oppnådd tilstrekkelig tillit slik at en godkjenning kan finne sted. Slik evaluering fordrer NSMs tilgang til dokumentasjon og implementasjon.

Dersom NSM godkjenner et kryptosystem gjøres dette for et spesifikt formål i tråd med kryptosystemets funksjon og virkemåte, uavhengig av informasjonssystem, og med nasjonal virkning om ikke særskilte forhold, herunder forhold fremmet av søkende virksomhet, taler i mot dette. NSM fører kryptosystemet opp i en produktliste over godkjente høytillitskryptosystemer[7], der dets formål og sikkerhetsgraderingen det høyst kan beskytte framkommer. Tilknyttet listen vil det fremkomme hvilke krav NSM har gitt for kryptosystemenes implementering, bruk, drift og forvaltning.

Virksomheter som planlegger å anskaffe høytillitskryptosystemer som ikke allerede er godkjent av NSM, bør ha en dialog med NSM før anskaffelsen finner sted, for å avklare om NSM ser en vei fram mot et positivt godkjenningsvedtak for det aktuelle kryptosystemet[8].

Kryptosystemer som skal beskytte høygradert informasjon i norske informasjonssystemer som også skal behandle Nato-informasjon sikkerhetsgradert NATO SECRET eller høyere, må være godkjent av Natos militærkomité, jf. *Security Within the North Atlantic Treaty Organization (NATO)*, C-M(2002)49-REV1.

4.2. Særskilt for kommersielle kryptosystemer

For kommersielle kryptosystemer viser NSM til virksomhetsikkerhetsforskriften §§ 16 og 17. NSM anbefaler bruk av allment tilgjengelige produkter som implementerer kryptoalgoritmer som er anbefalt i

[7] Jf. forskrift om kryptosikkerhet § 2, sjuende ledd. Listen er sikkerhetsgradert, og er tilgjengelig fra NSM ved tjenstlig behov.

[8] Jf. forskrift om kryptosikkerhet § 2, femte ledd, bokstav b, og virksomhetsikkerhetsforskriften § 27, fjerde ledd, andre punktum.

NSM Cryptographic Recommendations[9], og som har gjennomgått nødvendig evaluering og sertifisering.

Markedet for kommersielle kryptosystemer er mer variert og har på mange områder en høyere teknologisk utviklingstakt enn det tilsvarende markedet for høytillitskryptosystemer. NSM utsteder derfor ikke informasjonssystemuavhengige produktgodkjenninger for slike kryptosystemer, men godkjenner heller bruken av dem i konteksten av det konkrete informasjonssystem der de skal beskytte sikkerhetsgradert informasjon. Dette gjøres i forbindelse med godkjenningsmyndighetens godkjenning av informasjonssystemet.

Tillitsnivået et kryptosystem må være evaluert til og sertifisert for avhenger av kryptosystemets rolle i et konkret informasjonssystem, og må vurderes iht. risiko, funksjon, og virksomhetens plikt til å etablere et forsvarlig sikkerhetsnivå. NSM anser at et tilstrekkelig tillitsnivå vanligvis kan oppnås ved evaluering iht. Common Criteria EAL4, EAL5 eller etter en anerkjent Protection Profile, ISO/IEC 19790 Level 2 eller Level 3, eller FIPS PUB 140-3 Level 2 eller Level 3.

Dersom kryptosystemer benyttes i et informasjonssystem på en måte som medfører at bestemmelser i virksomhetsikkerhetsforskriften §§ 16 og 17 ikke kommer til anvendelse, anbefaler NSM likevel bruk av evaluerte og sertifiserte løsninger.

Kryptosystemer som skal beskytte lavgradert informasjon i norske informasjonssystemer som også skal behandle Nato-informasjon sikkerhetsgradert NATO RESTRICTED bør på forhånd være godkjent til dette formålet av et Nato-land.

5. Godkjenning av informasjonssystem

Skjermingsverdige informasjonssystemer som behandler sikkerhetsgradert informasjon skal være godkjent av godkjenningsmyndigheten før bruk, jf. sikkerhetsloven § 6-3. NSMs Veileder for godkjenning av informasjonssystem beskriver krav til, og prosesser for slik godkjenning.

Sikkerhetsloven §§ 5-3[10] og 6-2[11] stiller krav til virksomhetens etablering av et forsvarlig sikkerhetsnivå når den håndterer risiko i relasjon til hhv. skjermingsverdig informasjon og skjermingsverdige informasjonssystemer. Implementering av et kryptosystem vil ofte være et sikkerhetstiltak som bidrar, sammen med andre tiltak, til å redusere risiko og etablere et forsvarlig sikkerhetsnivå.

[9] Tilgjengelig på NSMs internettsider.

[10] Jf. virksomhetsikkerhetsforskriften §§ 22 og 34.

[11] Jf. virksomhetsikkerhetsforskriften § 49.

For informasjonssystemer som benytter kryptosystemer som sikringstiltak, tilkommer det krav for sikker bruk og forvaltning av kryptosystemene på en måte som understøtter sikkerhetsmålene til informasjonssystemet. Dette kapittelet omhandler disse kravene.

NSM forventer at virksomheter som har eller bruker kryptosystemer ser kryptosikkerhet i sammenheng med det øvrige IKT-sikkerhetsarbeidet som følger av virksomhetens styringssystem[12]. Det er avgjørende for virksomhetens evne til å etablere og opprettholde et forsvarlig sikkerhetsnivå å se kryptosikkerhet i sammenheng med øvrig informasjons- og informasjonssystemsikkerhet i virksomheten. Sikkerhetstruende hendelser relatert til kryptosystemer kan ha katastrofal konsekvens for virksomhetens informasjons- og informasjonssystemsikkerhet, noe som igjen skader nasjonale, og ofte alliertes, sikkerhetsinteresser.

Høytillitskryptosystemer bør benyttes for å beskytte lavgradert informasjon i informasjonssystemer der konsekvensene ved kompromittering er større enn sikkerhetsgraden i utgangspunktet skulle tilsi. En slik vurdering må ta utgangspunkt i risikoanalysen som virksomheten har utført etter virksomhetsikkerhetsforskriften § 12 og vil typisk være aktuell for store informasjonssystemer av strategisk nasjonal betydning. Bruk av høytillitskryptosystemer medfører krav om etablering av kryptosikkerhetsorganisasjon og nøkkelhåndteringsplan som for beskyttelse av høygradert informasjon[13].

Virksomheter som skal etablere et skjermingsverdig informasjonssystem skal informere NSM om dette[14]. I denne dialogen kan virksomheten be om råd vedr. valg av kryptosystem.

5.1. Implementering og forvaltning

Kryptosystemer som skal inngå som sikkerhetstiltak i informasjonssystemer må implementeres på en måte som ikke undergraver sikkerhetsfunksjonaliteten som kryptosystemet tilbyr. Det er viktig at kryptosystemer implementeres som del av informasjonssystem innen de rammer som gis i kryptosystemenes evaluerings- og sertifiseringsdokumentasjon, samt brukermanualer og andre føringer fra leverandør. Det er videre viktig at utviklere, brukere, driftspersonell og annet involvert personell tilføres nødvendig kompetanse slik at dette implementeres og opprettholdes i praksis.

For høytillitskryptosystemer angir NSM akseptert bruksformål, og stiller kryptosystemspesifikke krav til implementering, bruk, drift og forvaltning i forbindelse med godkjenning av dem.

Videre stiller forskrift om kryptosikkerhet en rekke krav til sikker forvaltning av kryptoutstyr og kryptonøkler som inngår i høytillitskryptosystemer. Disse kravene fordrer etablering av en kryptosikkerhetsorganisasjon bestående av særskilt autorisert og kvalifisert personell som skal ivareta virksomhetens

[12] Jf. sikkerhetsloven § 4-1.

[13] Merk at kostnader ved sikkerhetstiltak skal stå i et rimelig forhold til det som oppnås ved tiltaket, jf. virksomhetsikkerhetsforskriften § 15, andre ledd, men dersom risikoanalysen tilsier bruk av høytillitskryptosystemer må dette medføre behov for høy grad av tillit til personell og prosedyrer, ikke bare teknologi.

[14] Jf. virksomhetsikkerhetsforskriften § 50.

kryptosikkerhet, herunder forvaltning av kryptoutstyr og kryptonøkler, på tvers av virksomhetens informasjonssystemer.

Virksomheten må utpeke personell eller organisasjon ansvarlig for den tekniske forvaltning av virksomhetens kryptosystemer[15]. I dette ansvaret ligger kontinuerlig oppfølging av sikkerhetsoppdateringer, reparasjon og øvrig teknisk vedlikehold av kryptosystemene så lenge de er i bruk, og forsvarlig avhending når bruk skal opphøre. Ofte vil det være nødvendig å etablere vedlikeholdsavtaler med leverandører av kryptosystemer for å ivareta et slikt ansvar med tilstrekkelig kvalitet og over tid.

For hvert kryptosystem som inngår i et informasjonssystem, vil informasjonssystemets godkjenningsmyndighet[16] vurdere om kryptosystemet er planlagt driftssatt på en måte som understøtter informasjonssystemets sikkerhetsmål og forsvarlige sikkerhetsnivå. Godkjenningsmyndigheten vil herunder vurdere virksomhetens plan for opplæring av personell som kommer i befatning med kryptosystemet, og virksomhetens plan for å vedlikeholde kryptosystemet i dets levetid. For høytillitskryptosystemer vurderer godkjenningsmyndigheten om kryptosystemets implementering, bruk, drift og forvaltning er i samsvar med krav framsatt av NSM.

5.2. Kryptonøkkelhåndtering

Bruk av kryptosystemer for å beskytte skjermingsverdig informasjon under transport eller lagring medfører at den krypterte informasjonen har redusert, helst ingen, verdi for en motstander som får tak i den. Kryptonøklene som medvirker i kryptosystemet får derimot en verdi tilsvarende all den informasjonen som kryptosystemet har beskyttet og skal beskytte. Kryptonøklene har høy verdi og er tilsvarende utsatt for høy risiko. Sikker håndtering av kryptonøkler blir derfor avgjørende for virksomhetens faktiske evne til å håndtere risiko og etablere et forsvarlig sikkerhetsnivå ved å bruke av kryptosystemer.

Alle informasjonssystemer skal ha en kryptonøkkelhåndteringsplan. En slik plan må identifisere kryptonøkler i bruk av kryptosystemene som beskytter informasjonssystemet, og detaljere alle sider ved håndteringen av disse kryptonøklene, herunder de prosedyrer og personellmessige og tekniske tiltak som virksomheten har etablert eller skal etablere for å håndtere risiko kryptonøkler er utsatt for.

Forskjellige typer kryptosystemer vil ha forskjellige teknikker for hvordan kryptonøkler benyttes i systemet. En kryptonøkkelhåndteringsplan må møte den risiko som kryptonøkler utsettes for innenfor rammen av de konkrete kryptosystemer som er i bruk for å beskytte et konkret informasjonssystem.

En kryptonøkkelhåndteringsplan må utpeke personell eller organisasjon ansvarlig for den sikkerhetsmessige forvaltning av informasjonssystemets kryptonøkler i nøklenes livsløp, og som kan fungere

[15] For noen typer utstyr som inngår i høytillitskryptosystemer kan det finnes en nasjonal hovedforvalter utpekt av NSM, jf. forskrift om kryptosikkerhet § 3. Dette fritar ikke den enkelte virksomhet fra å sørge for teknisk forvaltning av utstyr som virksomheten bruker eller eier. Virksomheten bør i slike tilfeller koordinere forvaltning med den nasjonale hovedforvalteren.

[16] Godkjenningsmyndighet bestemmes av virksomhetsikkerhetsforskriften § 51.

som kontaktpunkt ved sikkerhetstruende hendelser. Hendelser som truer kryptosikkerheten må håndteres sammen med virksomhetens øvrige informasjons- og informasjonssystemsikkerhetsmiljøer. Denne nødvendige samhandlingen må reflekteres i virksomhetens styringssystem for sikkerhet.

For høytillitskryptosystemer oppstiller forskrift om kryptosikkerhet en rekke konkrete krav til virksomhetens organisering av dette arbeidet, herunder hvordan virksomhetens kryptosikkerhetsorganisasjon skal forvalte kryptonøkler. Dette regelverket må også følges for informasjonssystemer som skal beskytte lavgradert informasjon med høytillitskryptosystemer. Den samme risikovurderingen som medfører behov for økt tillit til kryptosystemene som brukes, må også føre til et behov for økt tillit til kryptonøkkelhåndteringen. Uavhengig av om informasjonssystemet skal behandle Nato-informasjon anbefaler NSM dessuten at relevante Nato-doktriner innen kryptonøkkelhåndtering implementeres[17] for å sikre mulighet for alliert samhandling i hele krisespennet.

Kryptonøkler for høytillitskryptosystemer skal iht. forskrift om kryptosikkerhet § 2, tredje ledd produseres av NSM, så fremt ikke annet er eksplisitt avtalt med NSM[18].

Eiere av informasjonssystemer som skal bruke høytillitskryptosystemer bør dokumentere hvordan dette regelverket møtes ved å inkludere en kryptonøkkelhåndteringsplan i søknad om godkjenning etter sikkerhetsloven § 6-3.

For kommersielle kryptosystemer bør produktets brukermanual og andre føringer fra leverandøren følges, også for nøkkelhåndtering. Samtidig bør virksomheten vurdere de råd som gis i *NSM Cryptographic Recommendations* og NIST SP 800-57 *Recommendation for Key Management* når virksomheten etablerer en kryptonøkkelhåndteringsplan.

Eiere av informasjonssystemer som skal bruke kommersielle kryptosystemer bør dokumentere hvordan disse rådene møtes ved å inkludere en kryptonøkkelhåndteringsplan i søknad om godkjenning etter sikkerhetsloven § 6-3.

6. Øvrige krav til godkjenninger

Forskrift om kryptosikkerhet har flere bestemmelser der NSM skal godkjenne aspekter ved virksomhetens kryptosikkerhet. Etter forvaltningspraksis anser NSM bestemmelsene i forskrift om kryptosikkerhet å gjelde for virksomheters implementering, bruk, drift og forvaltning av høytillitskryptosystemer, til tross for at dette ikke eksplisitt er en avgrensning i forskriften unntatt for visse enkeltbestemmelser.

[17] Relevante doktriner er nyeste revisjoner av SECAN-publikasjonene SDIP-293, *Instructions for the Control and Safeguarding of NATO Cryptomaterial*, og SDIP-36, *Controlling Authorities for Keying Material and Management of Off-Line Cryptosystems*. Disse publikasjonene er sikkerhetsgradert NATO RESTRICTED, og er tilgjengelige fra NSM ved tjenstlig behov.

[18] Jf. forskrift om kryptosikkerhet § 2, femte ledd bokstav f, og § 2, sjette ledd. Merk at der § 2 sjette ledd henviser til femte ledd nummer 4 til 6 menes femte ledd bokstav d, e og f.

Etter forskrift om kryptosikkerhet § 2, femte ledd, bokstav a, skal NSM godkjenne kryptoutstyr til beskyttelse av informasjon gradert KONFIDENSIELT eller høyere. NSM forstår det slik at dette tilsvarer bestemmelsen i sikkerhetsloven § 5-6 første ledd, siden vi ser *kryptoutstyr* som en undermengde av *kryptosystem*, jf. denne veilederens kapittel 4.

Etter forskrift om kryptosikkerhet § 2, femte ledd, bokstav b, skal NSM godkjenne anskaffelse av kryptomateriell for beskyttelse av informasjon gradert KONFIDENSIELT eller høyere. Dette ivaretas ved at virksomhet som skal anskaffe kryptoutstyr eller kryptosystem fører en dialog med NSM i forkant av at anskaffelsen forpliktes. Bestemmelsen er ment å redusere usikkerhet for virksomheten i en senere godkjenningsprosess.

Etter forskrift om kryptosikkerhet § 2, femte ledd, bokstav c, skal NSM godkjenne bruk av kryptoutstyr og kryptosystemer, og kryptosikkerheten i den enkelte virksomhet. I dette inngår flere aspekter rundt implementering, bruk, drift og forvaltning av kryptosystemer. Mange av disse aspektene godkjennes per informasjonssystem, jf. denne veilederens kapittel 5. Det som gjenstår er virksomhetens mer generelle kryptosikkerhet, som skal ivaretas på tvers av informasjonssystemer ved hjelp av en kompetent kryptosikkerhetsorganisasjon. Virksomheten må etablere kryptosikkerhetsorganisasjon iht. forskrift om kryptosikkerhet, og anmode om at NSM godkjenner virksomhetens kryptosikkerhet.

Etter forskrift om kryptosikkerhet § 11 skal NSM godkjenne «programmer for utdanning.» Dette innebærer at NSM skal godkjenne de programmer som virksomheten etablerer for å gi nødvendig opplæring til virksomhetens kryptosikkerhetsorganisasjon og til de som skal implementere, bruke, drifte, og forvalte kryptosystemer.

Etter forskrift om kryptosikkerhet § 40 skal NSM godkjenne installasjon av kryptoutstyr. Installasjon av kryptoutstyr skal gjøres iht. de krav som NSM har satt i forbindelse med godkjenning av kryptosystemet, samt føringer i brukermanualer. Virksomheten bør føre en dialog med NSM og godkjenningsmyndigheten om hvorvidt det er nødvendig at hver enkelt installasjon av kryptoutstyr må saksbehandles for seg, eller om installasjoner med lav risiko og som ikke fraviker fra etablerte krav kan anses som godkjente på linje med informasjonssystemet for øvrig.

Etter forskrift om kryptosikkerhet § 36 skal NSM godkjenne flere aspekter ved etablering og bruk av *kryptorom*. Kryptorom er kun påkrevd ved installasjon av kryptoutstyr som det stilles krav til kryptoautorisasjon for å bruke, jf. § 35 første ledd. Dette gjelder i hovedsak kryptoutstyr uten godkjent manipulasjonssikring, samt eldre typer kryptosystemer. Slikt utstyr er ikke lenger i bruk, og bestemmelsene i § 36 kommer derfor vanligvis ikke til anvendelse. Bestemmelsen kan anses som en anakronisme med bakgrunn i de siste tiårs utvikling innen kryptoteknologi. NSM anbefaler likevel at virksomheter vurderer å legge kravene i § 36 til grunn ved etablering av lokaler for høygradert IKT-infrastruktur eller lokaler for annen infrastruktur som er utsatt for særlig høy risiko.

7. Endringslogg

Dette er første utgivelse av denne veilederen. Fremtidige revisjoner vil beskrives kort under dette kapittelet.

Vedlegg A: Sjekkliste

Vedlegget omhandler nødvendig informasjon godkjenningsmyndigheten trenger for å kunne saksbehandle en søknad om godkjenning for et informasjonssystem som benytter kryptosystem som sikkerhetstiltak.

Det er avgjørende at den som søker godkjenning ser på kryptosystemet som en integrert del av informasjonssystemet, og beskriver kryptosystemet sammen med informasjonssystemet for øvrig i en systembeskrivelse. Kryptosystemet må integreres i informasjonssystemet teknisk men også organisatorisk.

Basert på et kryptosystems sertifisering (og godkjenning etter § 5-6), så vurderes kryptosystemets integrasjon i informasjonssystemet som en evaluert og sertifisert komponent som tilfredsstiller krav i virksomhetsikkerhetsforskriften §§ 16 og 17. Kryptosystemer er å anse som sikkerhetstiltak i et skjermingsverdig informasjonssystem.

For høytillitskryptosystemer er det særlig viktig at implementering, bruk, drift og forvaltning av kryptosystemet er i henhold til de rammer som foreligger fra sikkerhetsmyndighetens godkjenning etter sikkerhetslovens § 5-6. Dette må søker klart få fram i sin søknad, og godkjenningsmyndigheten må ettergå dette.

For kommersielle kryptosystemer vil det antakelig ikke foreligge en informasjonssystemuavhengig produktgodkjenning. Implementering, bruk, drift og forvaltning må beskrives ut fra bruks- og installasjonsmanualer, sertifiseringsdokumentasjon og anerkjent beste praksis. Godkjenningsmyndigheten må vurdere om dette reduserer risiko og etablerer et forsvarlig sikkerhetsnivå, for deretter å videreformidle søknad om godkjenning av kryptosystem etter § 5-6 til NSM.

Under følger en sjekkliste som bør leses sammen med NSMs Veileder for godkjenning av informasjonssystem kapittel 2.2.1 som veileder i utforming av en systembeskrivelse. Systembeskrivelsen skal beskrive informasjonssystemets funksjon[19] og operative miljø[20] som er ment å avdekke et beskyttelsesbehov som legges til grunn av godkjenningsmyndigheten ved vurdering av valgte sikkerhetstiltak.

Siden kryptosystemer er et teknisk tiltak med organisatoriske konsekvenser, må kryptosystemets implmentering, bruk, drift og forvaltning beskrives som del av den tekniske løsningen, som del av operative organisatoriske forhold, og som sikkerhetstiltak som møter et beskyttelsesbehov.

[19] Herunder informasjonssystemets formål, verdivurdering eller klassifisering, teknologi, sammenkoblinger og forbindelser, konfigurasjon og tjenester.

[20] Herunder informasjonssystemets fysiske omgivelser, elektroniske omgivelser, menneskelige omgivelser, og organisatoriske forhold innen systemdrift og –vedlikehold, regelverksutvikling, sikkerhetsgodkjenning, og oppfølging av forebyggende sikkerhetsarbeid for øvrig.

- **Systembeskrivelsen: Beskrivelse av funksjon**
    - Kryptosystemets anvendelse og oppsett beskrives under *Teknologi* og *Konfigurasjon*, og under *Tjenester* dersom kryptosystemet tilbyr brukerorienterte tjenester.
        - Valg av kryptosystem bør beskrives i lys av informasjonssystemets formål den informasjonen som informasjonssystemet skal behandle. Informasjonssystem som må benytte høytillitskryptosystemer må velge kryptosystem fra NSMs liste over godkjente produkter.
- **Systembeskrivelsen: Beskrivelse av operativt miljø**
    - Virksomhetens evne til å håndtere sikkerhetstruende hendelser i forbindelse med informasjonssystemet beskrives under *Organisatoriske forhold* på en slik måte at det klart framkommer hvordan kryptosikkerhet og informasjonssikkerhet for øvrig koordineres for informasjonssystemet.
    - Virksomhetens evne til forvaltning, drift og vedlikehold av kryptosystemet beskrives under *Organisatoriske forhold*. For hvert kryptosystem i bruk må det framkomme
        - At virksomheten evner å vedlikeholde kryptosystemet over tid, for eksempel ved at man har inngått en vedlikeholdsavtale med leverandøren.
        - At virksomheten evner å etablere nødvendig kompetanse hos sitt personell som skal implementere, bruke eller drifte kryptosystemet.
    - Spesielt for informasjonssystemer som benytter høytillitskryptosystemer:
        - Virksomhetens kryptosikkerhetsorganisasjon og dens befatning med informasjonssystemet, herunder dets kryptosystemer, beskrives under *Organisatoriske forhold.* Det må framkomme at virksomhetens kryptosikkerhetsorganisasjon er godkjent av NSM, og at relevant personell har kryptokvalifisering og kryptoautorisasjon.
        - Informasjonssystemets kryptonøkkelhåndteringsplan beskrives under *Organisatoriske forhold*, eventuelt vedlegges systembeskrivelsen. Vesentlige forhold knyttet til forvaltning av kryptonøkler og tildeling av dem må framkomme for hvert kryptosystem i bruk, herunder:
            - Organisasjon eller personell som innehar det kryptosikkerhetsmessige ansvaret for kryptonøkler (jf. rollene *kontrollerende myndighet* iht. forskrift om kryptosikkerhet og *Controlling Authority* iht. SDIP-293 og SDIP-36).
            - Identifisering av kryptonøkler som skal brukes av informasjonssystemet, herunder med korttittel eller korttitler hvis tilgjengelig.
            - Tekniske og forvaltningsmessige forhold rundt kryptonøkkelhåndtering, som nøkkel- og sertifikatlevetider (kryptoperioder) tilpasset risiko, distribusjonskanaler, prosedyrer for gjenoppretting etter sikkerhetstruende hendelser, rapporteringskanaler, oppbevaring, bruk og destruksjon.
    - Spesielt for informasjonssystemer som benytter kommersielle kryptosystemer:
        - Informasjonssystemets kryptonøkkelhåndteringsplan beskrives under *Organisatoriske forhold*, eventuelt vedlegges systembeskrivelsen. Vesentlige forhold knyttet til forvaltning av kryptonøkler og tildeling av dem må framkomme for hvert kryptosystem i bruk, herunder:
            - Organisasjon eller personell som innehar det kryptosikkerhetsmessige ansvaret for kryptonøkler eller PKIer i bruk av kryptosystemet.
            - Tekniske og forvaltningsmessige forhold rundt kryptonøkkelhåndtering, som nøkkel- og sertifikatlevetider (kryptoperioder) tilpasset risiko, distribusjonskanaler, prosedyrer for gjenoppretting etter sikkerhetstruende hendelser, rapporteringskanaler, oppbevaring, bruk og destruksjon.

For høytillitskryptosystemer må systembeskrivelsen i sum kunne gjøre det mulig for godkjenningsmyndigheten å fastslå om NSMs krav til implementering, bruk, drift og forvaltning, og for øvrig de krav som fremkommer i forskrift om kryptosikkerhet er møtt.

For kommersielle kryptosystemer må systembeskrivelsen tilsvarende kunne gjøre det mulig for godkjenningsmyndigheten å vurdere om kryptosystemet benyttes iht. de rammer satt av produsenten og sertifiserende myndighet.

Jf. Veileder for godkjenning av informasjonssystem, så skal beskyttelsesbehovet som utledes fra systembeskrivelsen, møtes med sikkerhetstiltak. Sikkerhetstiltakene beskrives også i søknad om godkjenning, herunder hvordan de implementeres og kontrolleres.

Implementering av kryptosystem er et slikt sikkerhetstiltak, og beskrives derfor som det. Kryptosystemets sertifiseringsstatus eller tidligere informasjonssystemuavhengige godkjenning etter sikkerhetsloven § 5-6 oppgis her.

Nasjonal sikkerhetsmyndighet

Postboks 814
1306 Sandvika

postmottak@nsm.no
www.nsm.no