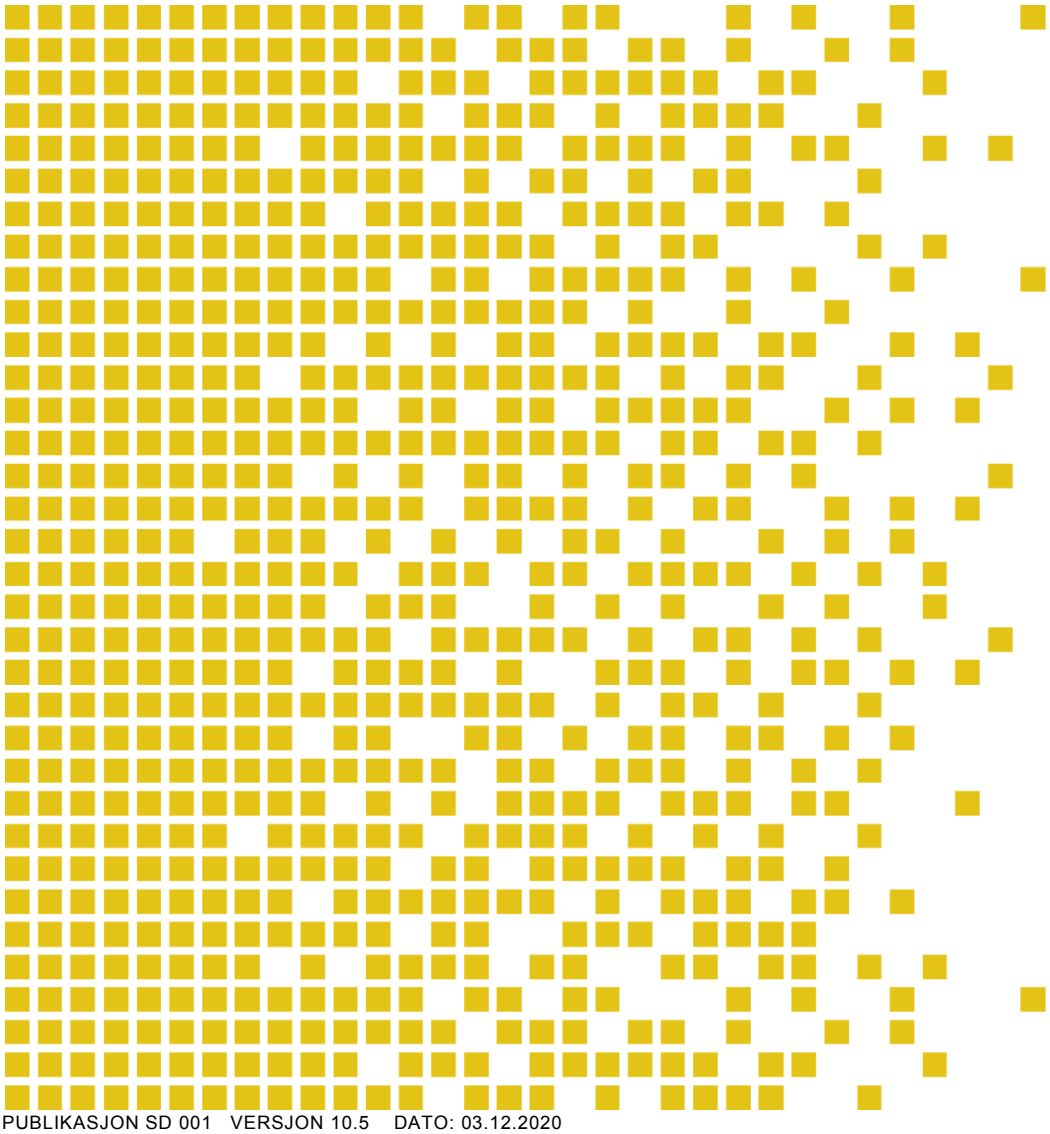
SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

Den norske sertifiseringsordningen

Evaluering og sertifisering av IT-sikkerhet



PUBLIKASJON SD 001 VERSJON 10.5 DATO: 03.12.2020

SERTIT, P.O.Box 814, N-1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Internet: www.sertit.no

Dokumenthistorie

Versjon	Dato	Skrevet av	Godkjent
10.0	27.05.2016	LB	~~HRF~~
10.0 rev. 1	25.07.2017	LB	~~KSB~~
10.2	02.11.2017	LB	JAA
10.3	20.02.2018	LB	JAA
10.4	20.02.2018	LB	JAA
10.5	03.12.2020	LB	HN

Innhold

Definisjon av IT-sikkerhet

For å gi en entydig forståelse av hva IT-sikkerhet handler om og brukes i dette dokumentet, er det nedenfor gitt en definisjon av seks sentrale begreper; autentisitet, tilgjengelighet, integritet, konfidensialitet, tillit og ansvarlighet. Forskrift om informasjonssikkerhet [1] gir mer utfyllende definisjon av informasjonssystemsikkerhet og tilhørende tiltak.

- **Autentisitet** (Sikre at brukere er identifisert og autentisert før det gis tilgang til data og tjenester. Introduksjon av falske data og tjenester skal forhindres),
- **Tilgjengelighet** (Sikre at informasjon og dataressurser er tilgjengelig for autoriserte brukere til rett tid og i rett form),
- **Integritet** (Sikre at informasjon og dataressurser er korrekt og ikke blir endret eller ødelagt av uvedkommende),
- **Konfidensialitet** (Sikre at informasjonen ikke blir kjent for uvedkommende, og at dataressurser beskyttes mot uønsket bruk),
- **Tillit** (Systematisk kontroll av at sikkerhetstiltak er korrekt implementert og ivaretar sikkerheten på en effektiv og hensiktsmessig måte),
- **Ansvarlighet** (Sørge for at sikkerhetsrelevante hendelser detekteres og registreres, slik at bruker kan holdes ansvarlig. Dette punktet omfatter også ikke-benekting).

IT-sikkerhet er med andre ord både tiltak og virkemidler for å beskytte informasjon som lagres, behandles og kommuniseres i IT-systemer og beskyttelse av selve dataressursene. Sertifisering er en metode for å vurdere og angi tillit til IT-sikkerhet. Det er denne forståelsen av IT-sikkerhet som gjelder i dette dokumentet.

1 Innledning

Den raske IT-utviklingen, tiltakende bruk av IT og økt avhengighet av IT i samfunnet, har de seneste årene også synliggjort samfunnets sårbarhet ved sikkerhets svikt i IT-systemer. Følgelig er det behov for bedre forhåndskunnskap om styrker og svakheter i ulike IT-produkter. Det kan også være et behov for å kunne sammenlikne sikkerhetsegenskaper i et mangfold av ellers like produkter. Mangel på informasjon eller misvisende informasjon kan blant annet føre til feilinvesteringer eller for lav IT-sikkerhet.

Det foreligger minst tre alternativer for å vurdere IT-sikkerhet:

- Det første alternativet er å stole på leverandørens vurderinger,
- Det andre alternativet er å foreta egne tester og vurderinger,
- Det tredje alternativet er å bruke en kompetent offentlig uavhengig tredjepart.

Det første alternativet kan være komfortabelt, men gir ingen forsikringer om at det er anvendt beste praksis for design og implementering av sikkerhetsløsningen og at relevante svakheter, feil og mangler er oppdaget og korrigert. Kunden kan derfor løpe en risiko for at IT-plattformen ikke gir ønsket nivå av beskyttelse.

Det andre alternativet er både tidkrevende og komplisert. I et samfunnsmessig perspektiv er det lite optimalt at hver enkelt skal bruke ressurser på egne vurderinger, som kanskje også er basert på ulike kriterier og som ikke nødvendigvis gir tilstrekkelig visshet om sikkerhetsnivået.

Det tredje alternativet er en uhildet tredjepartsvurdering etter internasjonalt anerkjente standarder. I et samfunnsmessig perspektiv er det mer rasjonelt at vurderingen skjer én gang ett sted og at resultatet deretter kan anerkjennes av mange.

For ansvarlige i både offentlig og privat sektor eller for privatpersoner, er det viktig å få stadfestet sikkerhetsnivået på IT-løsningen. I tillegg er det også av betydning å kunne ha tillit til at IT-produktet har gjennomgått en uhildet vurdering av en nøytral faginstans. Dette er oppnådd gjennom etableringen av sertifiseringsordningen.

Hensikten med den norske sertifiseringsordningen er å tilby tjenester som bygger opp under det tredje alternativet, og fortsettelsen av dokumentet handler derfor utelukkende om tredjepartsordninger for sertifisering av IT-sikkerhet.

Norge er medlem av et internasjonalt arrangement *"Common Criteria Recognition Arrangement"* (CCRA), jf kapittel 1.1 og [7], og en europeisk avtale *"Mutual Recognition Agreement of Information Technology Security Evaluation Certificates"* (SOGIS-MRA), jf. kapittel 1.1 og [24].

Medlemsnasjonene har forpliktet seg til å anerkjenne sertifikater som er utstedt av kvalifiserte sertifiseringsmyndigheter. IT-produkter skal

sikkerhetsevalueres og sertifiseres i henhold til de internasjonale evalueringskriteriene *Common Criteria* (CC) [3], [4] og [5], svarende til ISO/IEC 15408 [12] og metodikken *Common Evaluation Methodology* (CEM) [6], svarende til ISO/IEC 18045 [14].

Nasjonal sikkerhetsmyndighet (NSM) er avtalepart i CCRA og SOGIS MRA. Sertifiseringsmyndigheten for IT sikkerhet (SERTIT) er gitt forvaltningsansvaret for ordningene. Det er også SERTIT som utformer rammevilkår for ordningene og utfører sertifisering av IT-sikkerhet i Norge.

Formålet med ordningene er blant annet å dekke myndighetenes og industriens behov for en kostnadseffektiv og rasjonell sikkerhetsevaluering og sertifisering av IT-produkter.

Utgangspunktet for å sette i verk en sertifiseringsprosess kan være slik som:

- leverandør ønsker å styrke sin markedsmessige posisjon,
- myndighetenes og næringslivets behov for tillit til at sikkerhetskrav er tilfredsstilt,
- krav til systemutvikler om å tilfredsstille gitte betingelser i en bestemt kontrakt,
- anskaffer av et produkt må følge bedriftens egne sikkerhetskrav, bransjekrav eller sikkerhetskrav gitt i medhold av lov eller forskrift.

Ytterligere informasjon om sertifiseringsordningene eller kommentarer kan fås ved henvendelse til/rettes til:

Sertifiseringsmyndigheten for IT-sikkerhet (SERTIT)
Postboks 814
1306 SANDVIKA

Besøksadresse: Langkaia 1, Oslo

Telefon: 67 86 40 00

Internett: sertit.no

1.1 Rammer

SERTITs forankring og bemyndigelse er gitt i to dokumenter fra Nærings- og handelsdepartementet (NHD) av 01.02.1999 og 14.04.1999, begge med referanse 98/4561-F-ITK eja/lem. For mer informasjon om grunnlaget for etableringen av ordning for sertifisering av IT-sikkerhet vises til vedlegg A.

Sertifiseringsordningene under SERTIT bygger på følgende internasjonale arrangement og avtale om gjensidig anerkjennelse av sertifikater:

- *"Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security"* (CCRA) [7],
- *"Mutual Recognition Agreement of Information Technology Security Evaluation Certificates"* (SOGIS MRA) [24].

Følgende nasjonale bestemmelser er sentrale for involverte parter under sertifiseringsordningen:

Lov om nasjonal sikkerhet (sikkerhetsloven) [22] med forskrifter og veiledninger,

- Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) [10],
- Lov om behandling av personopplysninger (personopplysningsloven) [15],
- Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (Beskyttelsesinstruksen) [1].

Alle SERTIT-dokumenter som er omtalt i dette dokumentet eller som er publisert på SERTITs internettsider inngår i rammevilkår for sertifiseringsordningen. Endringer i rammevilkårene blir publisert i henhold til gjeldende prosedyrer for ordningen.

1.2 Gjensidig anerkjennelse

Norge har forpliktet seg til å gjennomføre sikkerhetsevaluering og sertifisering i henhold til internasjonalt anerkjente standarder og metodikker slik disse er definert i CCRA [7] og SOGIS MRA [24].

CCRA og SOGIS MRA inneholder to sentrale elementer:

- Alle som deltar er forpliktet til å godkjenne sertifikater etter de regler som gjelder i henholdsvis CCRA og SOGIS MRA,
- Godkjenning av kvalifiserte sertifiseringsmyndigheter, *"Qualified Participants (QP)"* (CCRA) eller *"Compliant CB"* (SOGIS MRA).

I henhold til dette anerkjenner Norge sertifikater som er utstedt under CCRA og SOGIS MRA.

Norge har status som kvalifisert sertifiseringsmyndighet i CCRA og SOGIS MRA, noe som innebærer at de norske sertifikatene anerkjennes under disse ordningene.

Resten av dette dokumentet beskriver nærmere hvordan ordningene er innrettet, hvilke rammer som gjelder for sikkerhetsevaluering og sertifisering og hvordan selve prosessen gjennomføres.

2 Prinsipper for sertifiseringsordningen

Et sentralt formål med sertifiseringsordningen er å sikre et høyt og konsistent kvalitetsnivå i evalueringene. Følgende prinsipper er lagt til grunn for sertifiseringsordningen:

- Ordningen er åpen og tilgjengelig for alle som ønsker å søke om sertifisering,
- Evaluering og sertifisering skal gjennomføres på en objektiv, upartisk og kosteffektiv måte,
- Sikkerhetsevalueringen gjennomføres av godkjente evalueringsfirma som driver etter vanlige forretningsmessige prinsipper,
- SERTIT godkjenner evalueringsfirma og fører ettersyn med virksomheten,
- SERTIT avgjør om TOE er egnet for sertifisering,
- Det tilbys gjensidig anerkjennelse av sertifikater som tilfredsstiller kriteriene under CCRA eller SOGIS MRA.

Evalueringsresultater skal være:

- Fremskaffet på bakgrunn av objektive vurderinger,
- Repeterbare og reproduserbare,
- Komplette og teknisk korrekte.

3 Organisering og ansvar

Den offentlige sertifiseringsordningen for IT-sikkerhet forvaltes av SERTIT, som er en del av Nasjonal sikkerhetsmyndighet (NSM).

Justis- og beredskapsdepartementet (JD) er budsjettansvarlig og bevilger midler til driften av NSM. SERTIT er derfor offentlig finansiert gjennom NSM.

Kapitlene 3.1 - 3.3 beskriver hvilke parter som inngår i sertifiseringsordningen, samt partenes hovedoppgaver og ansvarsområder.

3.1 SERTIT

SERTITs hovedoppgave som offentlig sertifiseringsmyndighet for IT-sikkerhet er primært å utstede sertifikater og sertifiseringsrapporter som angitt i mandat for SERTIT [21]. I tillegg er SERTIT ansvarlig for å utforme rammevilkår for ordningen, og se til at reglene følges av alle parter. SERTIT fører også ettersyn med hele evalueringsprosessen som utgjør grunnlaget for å kunne utføre sertifisering. SERTIT er dessuten godkjenningsmyndighet ved etablering av kommersielle evalueringsfirma under den offentlige sertifiseringsordningen.

For å ivareta oppgavene i SERTIT på en hensiktsmessig måte, herunder oppfylle de formelle kravene [7], [2], [24], [24], [25] og [26], slik at ordningen fungerer rasjonelt og effektivt, er virksomheten organisert på følgende måte:

Leder for SERTIT er hovedansvarlig for den daglige driften av ordningen. Sertifiseringsprosjekter tildeles en prosjektansvarlig som også er ansvarlig for utforming av sertifiseringsrapport og sertifikat. Kvalitetssystemet skal sikre at sertifiseringen blir utført på en tilfredsstillende måte.

3.2 Evalueringsfirma (EVIT)

Evalueringsfirma som utfører oppdrag for sertifiseringsordningen er underlagt SERTITs myndighetskontroll. Det betyr blant annet at SERTIT er ansvarlig for å godkjenne evalueringsvirksomheten, og senere verifisering av firmaet og alle evalueringsaktiviteter. Evalueringsvirksomheten er regulert gjennom en driftsavtale [20] mellom SERTIT og EVIT på bakgrunn av bestemmelsene i CCRA [7], SOGIS MRA [24] og nasjonale rammevilkår fastlagt av SERTIT. EVIT må blant annet ha gyldig akkreditering i henhold til ISO/IEC 17025 [25], og firmaet må tilfredsstille SERTITs krav til evalueringsfirma [17] for å kunne bli godkjent som firma og utøve evalueringsvirksomhet.

Evalueringsfirmaene utfører evaluering av PPer (evt cPPer) og/eller TOE på et forretningsmessig grunnlag og etter dokumenterte prosedyrer i henhold til internasjonale standarder [3], [4], [5], [6], [12], [14], arrangement [7] og avtale [24].

Informasjon om godkjente evalueringsfirmaer kan finnes på internettsidene sertit.no.

3.3 Eksterne parter

Et antall eksterne parter kan være involvert i en sertifiseringsprosess. De fleste av disse er enten sponsorer eller utviklere, men det kan også omfatte andre aktører. Nedenfor følger en detaljert beskrivelse av disse aktørene og noen retningslinjer for sertifiseringsprosessen.

3.3.1 Oppdragsgiver

Med oppdragsgiver menes en organisasjon eller person som anmoder om en sertifisering for et bestemt IT-produkt. Oppdragsgivers tilknytning til IT-produktet kan derfor være forskjellig, alt fra leverandør, anskaffer, agent som handler på oppdrag for en anskaffer, systemutvikler eller et konsortium som representerer flere utviklere eller leverandører.

I de tilfeller det er flere oppdragsgivere involvert, etableres en egen ledergruppe som opptrer som oppdragsgivernes kontaktpunkt.

De generelle rammevilkårene for sertifiseringsordningen vil kunne legge føringer på avtaleforholdet mellom oppdragsgiver og EVIT.

En oppdragsgiver kan også være utvikler av IT-produktet som skal sertifiseres. I mange tilfeller benytter utviklerne underleverandører, og rollen som utvikler behandles derfor nærmere i kapitlet nedenfor om utvikler.

3.3.2 Utvikler

Med utvikler menes den bedrift som produserer IT-produktet som skal sertifiseres. I de tilfeller utvikler ikke har rollen som oppdragsgiver, forutsettes et samarbeid mellom partene i forbindelse med evalueringsprosessen. Utvikler er ansvarlig for å gi nødvendig teknisk informasjon om IT-produktet til EVIT. Informasjonsbehovet omfatter blant annet tilgang til den dokumentasjon som er nødvendig for å gjennomføre sikkerhetsevaluering og sertifisering.

I enkelte tilfeller kan det være flere utviklere involvert i en sikkerhetsevaluering, noe som kan medføre problemer med å få tilgang på informasjon av betydning for sikkerhetsevalueringen. Denne typen samhandling forutsetter at nødvendige avtaler er inngått mellom partene på forhånd, se også kapittel 6.4 Avtale om sikkerhetsevaluering.

4 Generelle bestemmelser

Dette kapitlet inneholder noen sentrale bestemmelser om gjennomføring av sikkerhetsevaluering, rammevilkår for evalueringsvirksomhet, regler for publisering av informasjon og klager, tvister og tilbakemeldinger. For kvalifiserte evalueringsfirma eller firma med ambisjoner om å bli evalueringsfirma under den offentlige sertifiseringsordningen vises til nærmere detaljer i publikasjonen SD 003 [17].

4.1 Gjennomføring av sikkerhetsevaluering

Sertifiseringsordningen bygger på tillit og nøytral faglig vurdering.

Det kreves derfor blant annet en formell forhåndsgodkjenning fra SERTIT for å kunne påbegynne et evalueringsoppdrag under sertifiseringsordningen.

SERTIT fører ettersyn med at all sikkerhetsevaluering gjennomføres av en uhildet tredjepart og av kvalifisert personell.

4.2 Rammevilkår for evalueringsvirksomhet

SERTIT fastlegger rammevilkår for søknadsprosessen for å bli godkjent som EVIT. Dette omfatter blant annet etableringsvilkår, kriterier for utvalg og økonomiske forhold.

Intensjonen er at sertifiseringsordningen har tilstrekkelig kapasitet i forhold til etterspørselen i markedet, samt fungerer rasjonelt og effektivt.

Rammevilkårene for etablering av evalueringsvirksomhet er nærmere omtalt i dokumentet [17].

SERTIT vil informere de berørte partene om endringer i rammevilkårene.

4.3 Regler for publisering av informasjon

Følgende bestemmelser om publisering av informasjon om SERTIT, sertifiseringsordningen eller sertifiserte produkter gjelder for brukere av ordningen som blant annet oppdragsgivere, utviklere og EVIT:

- Partene må innhente forhåndsgodkjenning fra SERTIT ved utstedelse av pressemeldinger eller tilsvarende informasjon som vedrører sikkerhetsevalueringer og/eller sertifiseringer under ordningen,
- Partene kan ikke gi uttalelser i pressemeldinger, reklamemateriell eller tilsvarende som kan inneholde misvisende opplysninger om sikkerhetsevaluering og/eller sertifisering eller som på annen måte kan skade sertifiseringsordningen.

4.4 Klager, tvister og tilbakemeldinger

NSM ved SERTIT er første instans for håndtering av klager, tvister og tilbakemeldinger vedrørende sertifiseringsordningen. Alle enkeltvedtak kan påklages i henhold til forvaltningslovens bestemmelser. Ved klage eller ønske fra brukere av ordningen om endring i en avgjørelse SERTIT har fattet skal saken sendes skriftlig til NSM ved SERTIT. NSM ved SERTIT behandler saken og vurderer om avgjørelsen skal opprettholdes eller ikke. Dersom en part påklager en avgjørelse fattet av SERTIT, bringes saken til neste forvaltningsnivå som vurderer om klagen skal behandles. Alle faglige konflikter mellom oppdragsgivere, utviklere eller EVIT vedrørende ordningen skal tas opp med SERTIT.

5 Hva kan sertifiseres?

Det skilles mellom sertifisering av produkter *"Target of Evaluation"* (TOE), og sertifisering av kravprofiler uttrykt enten gjennom *"Protection Profile"* (PP) eller *"collaborative Protection Profile"* (cPP)[1].

5.1 Sertifisering av produkter (TOE)

Produkter som skal evalueres benevnes som TOE. TOE kan bestå av hele eller deler av et IT-produkt, samt tilhørende dokumentasjon for brukere- og administratorer. TOE beskriver gjerne en bestemt konfigurasjon eller et sett av ulike konfigurasjoner.

Produktets sikkerhetsfunksjoner defineres enten i form av *"Protection Profile"* (PP), *"collaborative Protection Profile"* (cPP), eller *"Security Target"* (ST). ST bør inneholde en eller flere PPer eller være basert på en cPP. For å kunne oppnå gjensidig anerkjennelse iht CCRA, er det krav om at ST må inneholde PP eller cPP. En formell beskrivelse av sikkerhetsfunksjonene er en av forutsetningene for å kunne påbegynne sertifisering av et produkt.

Evaluering og sertifisering av TOE utføres i henhold til gjeldende standard [3], [4], [5], [12], metodikk [6], [14] og prosedyrer.

5.2 Sertifisering av kravprofiler (PPer eller cPPer)

Kravprofiler uttrykt gjennom PPer eller cPPer beskriver generiske krav for et bestemt teknologiområde, som for eksempel en brannmur, et operativsystem eller en multifunksjonsskriver.

Forskjellene mellom en PP eventuelt cPP og en ST er at sistnevnte angir hvordan sikkerhetsfunksjonene er implementert og realisert i et bestemt produkt som eksempelvis en brannmur XY, versjon 1.0.

Evaluering og sertifisering av PPer og cPPer utføres i henhold til gjeldende standard [3], [4], [5], [12], metodikk [6], [14] og prosedyrer.

6 Forberedelser til sikkerhetsevaluering og sertifisering

Det er en rekke aktiviteter som inngår i den forberedende fasen frem til sikkerhetsevaluering og påfølgende sertifisering. Mesteparten av aktivitetene i denne fasen foregår uten sertifiseringsmyndighetens medvirkning. Det gjelder blant annet alle aktiviteter knyttet til produktutvikling og tilhørende dokumentasjon. Dette kapitlet beskriver aktiviteter som berører oppdragsgiver, evalueringsfirma og sertifiseringsmyndigheten.

[1] cPPer utformes av International Technical Communities (iTCs) i henhold til de gjeldende bestemmelser kunngjort på nettsidene til CCRA.

6.1 Forutsetninger for sikkerhetsevaluering

Alle sikkerhetsmessige forhold av betydning for sikkerhetsevalueringen skal identifiseres og inkluderes i en egen oversikt. Det kan blant annet omfatte minst følgende:

- TOE (maskinvare, fastvare, programvare),
- PP eller cPP,
- ST,
- teknisk dokumentasjon,
- bruker- og administratorguide,
- teknisk bistand fra utvikler,
- tilgang til utviklerens lokaler,
- tilgang til operativt miljø,
- verktøy.

Oppdragsgiver er ansvarlig for å utforme og kvalitetssikre *S*T, levere nødvendig dokumentasjon, samt skaffe teknisk bistand fra utvikler og tilgang til utviklers lokaler. Oppdragsgiver kan benytte ekstern bistand til utforming av ST.

ST skal forelegges både EVIT og SERTIT for vurdering med tanke på om det er tilstrekkelig og hensiktsmessig for å påbegynne sikkerhetsevaluering av TOE. Oppdragsgiver skal underrettes skriftlig om eventuelle problemer med å benytte fremlagte ST før evalueringen starter.

Forutsetningene må være tilfredsstilt for at sikkerhetsevalueringen skal kunne påbegynnes og gjennomføres. EVIT er ansvarlig for å dokumentere at forutsetningene er tilfredsstilt.

6.1.1 Varsling av oppdrag og fremdriftsplan for sikkerhetsevalueringen

EVIT er pålagt av SERTIT å varsle om nytt oppdrag i form av en *"Task Initiation Notice"* (TIN) der det anmodes om aksept til å gjennomføre sikkerhetsevaluering under sertifiseringsordningen. Dette skjer normalt etter forutgående undersøkelser av om forutsetningene for sikkerhetsevalueringen er tilfredsstilt.

TIN skal fremsendes til SERTIT for vurdering. Deretter avholdes normalt et startmøte mellom partene, etter forutgående gjennomgang av foreliggende dokumentasjon.

Hensikten med møtet er blant annet å sørge for at de involverte partene har tilstrekkelig kjennskap til TOE og en felles forståelse av omfanget av sertifiseringsprosessen.

6.1.2 Søknad om sertifisering

Oppdragsgiver skal sende søknad om sertifisering til SERTIT på et eget søknadsskjema [18] som kan lastes ned fra SERTITs internettsider.

Søknaden forplikter oppdragsgiver til å følge alle gjeldende regler i sertifiseringsordningen, og ikke utsette ordningen for ulovlige eller uønskede forhold eller på annen måte å skade ordningen.

For å sikre en effektiv sertifiseringsprosess anbefales det at TIN og søknaden med nødvendige vedlegg fremsendes samlet til SERTIT.

6.1.3 Opphavsrett og andre rettigheter

Det er normalt utvikleren som har opphavsrett til all informasjon om TOE, og det er derfor ingen automatikk i at oppdragsgiver har tilgang til denne typen informasjon. Spørsmål om opphavsrett bør derfor reguleres i en særskilt avtale mellom partene, se også kapittel 6.4 Avtale om sikkerhetsevaluering.

6.2 Godkjenning av sertifiseringsprosessen

SERTIT kan innvilge søknad om sertifisering dersom det er prinsipielt grunnlag for at sikkerhetsevaluering og sertifisering kan gjennomføres innen rammen av ordningen. Dette innebærer at følgende forhold må være tilfredsstilt:

- Sertifisering må være hensiktsmessig,
- De formelle kravene for sertifisering må være oppfylt,
- Sikkerhetsevaluering og sertifisering må kunne gjennomføres på en uhildet måte,
- Sikkerhetsevalueringen må være i samsvar med bestemmelsene i CCRA og/eller SOGIS-MRA, samt nasjonale bestemmelser,
- Det må fremgå av TIN at alle obligatoriske evalueringsaktiviteter er planlagt og at planene gjenspeiler en realistisk tidsramme. Planene må inneholde tilstrekkelig med ressurser, herunder kvantitet, kompetanse og nødvendig utstyr,
- Være stor grad av sannsynlighet for at alle evalueringsaktiviteter kan gjennomføres som planlagt.

Tilsagnet kan gis muntlig i møte med partene, men må senere bekreftes gjennom en formell uttalelse. Det skal bekreftes hvorvidt ST, PP/cPP, TOE, samt leveransene som angitt i TIN utgjør et tilstrekkelig grunnlag for den foreslåtte sikkerhetsevalueringen. Svar på søknaden blir sendt til alle involverte parter.

6.3 Konsulentbistand og forberedende aktiviteter til sikkerhetsevaluering

Bruk av konsulentbistand ved forberedelser til en sikkerhetsevaluering er ikke underlagt SERTITs kontroll, og er derfor en sak mellom oppdragsgiver og oppdragstaker. Bruk av konsulenter til utvikling eller forberedelser til evaluering er normalt uproblematisk så lenge firmaet kan bevise at kravene om uhildethet er tilfredsstilt. Forberedelser kan eksempelvis omfatte utforming av ST. EVIT bør derfor være nøye med å definere nivået på dets engasjement i problemløsningen for å sikre at firmaets uavhengige status ikke blir kompromittert og senere blir til hinder for en uhildet sikkerhetsevaluering.

Det anbefales at partene inngår en avtale som regulerer alle forhold ved bruk av konsulenter, blant annet for å sikre at nødvendig grad av uhildethet opprettholdes.

Ved tvil om uhildethet i saken bør EVIT kontakte SERTIT for å få de nødvendige avklaringer.

6.4 Avtale om sikkerhetsevaluering

Oppdragsgiver med behov for ekstern bistand til forberedelse av sikkerhetsevaluering eller som planlegger å gjennomføre sikkerhetsevaluering og senere sertifisering, oppfordres til å benytte seg av konkurransen i markedet gjennom å innhente tilbud fra flere evalueringsinstanser.

EVIT er pålagt av SERTIT å inngå en avtale med oppdragsgiver i forbindelse med oppdrag om sikkerhetsevaluering under sertifiseringsordningen. En slik bindende avtale skal foreligge før evalueringen kan påbegynnes. Det er opp til partene å definere detaljene i avtalen nærmere, men det anbefales at følgende forhold er inkludert:

- Behov for eventuell tilgang til tidligere evalueringsrapporter,
- Forhold knyttet til Forutsetninger for sikkerhetsevaluering som angitt i kapittel 6.1, blant annet tidsplaner, innsynsrett, krav til oppbevaring og eiendomsrett til informasjon,
- Alle forhold som vedrører bedriftssensitiv informasjon,
- Alle forhold ved bruk av konsulenter for å sikre at krav til uhildethet opprettholdes.

Det er oppdragsgivers ansvar å innhente skriftlig tillatelse fra utvikleren om å få tilgang til bedriftssensitiv informasjon, samt å gi avkall på sine egne rettigheter til evalueringsresultatene som kan kompromittere slik informasjon. SERTIT anbefaler at EVIT regulerer alle forhold vedrørende et eventuelt kontraktsbrudd i en egen avtale.

Det er SERTIT avgjør om EVIT er kvalifisert til å gjennomføre en sikkerhetsevaluering under sertifiseringsordningen. Avgjørelsen vil blant annet være basert på EVITs engasjement i konsulentvirksomheten og firmaets evne til å ivareta nødvendig uhildethet.

7 Sikkerhetsevaluering

Dette kapitlet beskriver hovedtrekkene i gjennomføringen av en sikkerhetsevaluering og samarbeidet mellom partene i prosessen. Kapitlet beskriver også hvilke trinn som inngår i utarbeidelsen av *"Evaluation Technical Report"* (ETR).

7.1 Gjennomføring

Den tekniske sikkerhetsevalueringen av TOE med tilhørende leveranser skal gjennomføres i henhold til godkjent fremdriftsplan. Sikkerhetsevalueringen utføres i henhold til gjeldende internasjonale bestemmelser gjennom CCRA, SOGIS MRA, øvrige nasjonale rammevilkår fastsatt av SERTIT og de internasjonale standardene CC og CEM. EVIT er pålagt å underrette SERTIT om all konsulentvirksomhet som er relatert til evalueringsoppdrag.

Eventuelle endringer i fremdriftsplanen skal godkjennes av SERTIT. Dette for å sikre at det foreslåtte arbeidet er tilstrekkelig, at planene er realistiske og at nødvendige ressurser er tilgjengelige. Sikkerhetsevalueringer uten fremdrift i 6 måneder kan termineres av SERTIT.

Både EVIT og SERTIT må forsikre seg om at integriteten av sikkerhetsevalueringen ikke er kompromittert. Med det menes at utvikleren ikke skal få mulighet til å påvirke resultatene eller hindre en nøyaktig og rettferdig presentasjon av resultatene fra sikkerhetsevalueringen.

7.1.1 Observasjonsrapporter og aktivitetsrapporter

EVIT skal løpende dokumentere aktiviteter og resultater fra sikkerhetsevalueringen i aktivitetsrapporter.

Dersom det avdekkes feil og mangler i TOE under sikkerhetsevalueringen, skal dette noteres i en observasjonsrapport, *"Evaluation Observation Report"* (EOR). EOR skal deretter formidles til oppdragsgiver og SERTIT for videre håndtering.

Oppdragsgiver skal besvare EOR skriftlig med detaljerte forslag til korrigering av påviste feil og mangler samt en tidsplan for eventuelle utbedringer. Utbedringene kan kreve justeringer i leveransene og kan ha konsekvenser for fremdriftsplanen. Synspunkter fra SERTIT kan fremmes gjennom en særskilt blankett for merknader (RF). EOR-er og eventuelle RF til EOR-er er saksdokumenter til fremdriftsmøtene, se kapittel 7.1.2. Prosessen går normalt i iterasjoner mellom partene helt til EOR-ene er løst. I de tilfellene det ikke er mulig å løse EOR vises til siste avsnitt i kapittel 7.1.2 Interaksjon.

7.1.2 Interaksjon

Det holdes fremdriftsmøter for sikkerhetsevalueringen mellom EVIT og oppdragsgiver. SERTIT kaller inn til og leder fremdriftsmøtene. Foruten

SERTIT skal EVIT, utvikler og oppdragsgiver delta. Møteplanen inngår som en del av fremdriftsplanen.

EVIT har normalt behov for å kommunisere direkte med utvikler om TOE, leveransene eller andre forhold. Det forutsettes i så fall at EVIT har inngått nødvendige avtaler med oppdragsgiver om slik kommunikasjon.

Behandling av EOR er en sentral del av fremdriftsmøtene. Løsningsforslag fra oppdragsgiver drøftes mellom partene med sikte på å finne akseptable løsninger på et tidligst mulig tidspunkt i evalueringsprosessen. EOR kan etter behov ferdigbehandles i møtet, og konklusjonen skal i så tilfelle tas inn i møtereferatet.

Dersom det ikke er mulig å rette opp feilen eller manglene og det vil ha konsekvenser for utfallet av sertifiseringsprosessen, skal SERTIT orientere oppdragsgiver om konsekvensene.

7.1.3 Ettersyn

SERTIT kan som ett ledd i ettersynsvirksomheten foreta nødvendige undersøkelser for å sikre at rammevilkårene for sikkerhetsevalueringen blir fulgt. SERTIT skal også gis mulighet til å være til stede under site-visit og testing.

7.2 Teknisk evalueringsrapport

Alle funn fra sikkerhetsevalueringen skal dokumenteres i en teknisk evalueringsrapport, ETR. Rapporten skal utformes etter gjeldende retningslinjer og på mal gitt av SERTIT. Rammeverket bygger på kravene i CCRA, anneks I, SOGIS MRA og CC/CEM. ETR utgjør sluttproduktet fra EVITs arbeid, og danner basis for sertifiseringsrapporten, *"Certification Report"* (CR).

Konklusjonene i ETR skal fastslå hvilke deler av evalueringskriteriene og sikkerhetskravene som er oppfylte eller ikke oppfylte samt angi tilstrekkelige bevis for dette.

7.2.1 Beskyttelse av informasjon og beskyttelsesmerking av ETR

Det må klart fremgå av rapporten dersom innholdet er å anse som forretningshemmeligheter, er det informasjon som ikke skal gjøres offentlig kjent. Dersom innholdet ikke kommer inn under sikkerhetsloven eller andre nasjonale bestemmelser, bør ETR merkes på en slik måte at det går klart frem at det er forretningshemmeligheter.

Når det gjelder beskyttelse av sensitiv informasjon i samband med sikkerhetsevalueringer og evalueringsrapporter for systemer i virksomheter som er underlagt sikkerhetsloven eller tilsvarende bestemmelser, skal all informasjon merkes og beskyttes i henhold til de til enhver tid gjeldende bestemmelser.

Utvikler kan ønske eller kreve å begrense oppdragsgivers adgang til bedriftssensitiv informasjon. EVIT er ansvarlig for at det er klart definert hvilken informasjon som skal beskyttes, og at sikkerhetsbestemmelsene følges. Både EVIT og SERTIT skal sørge for at oppdragsgiver ikke får tilgang til bedriftssensitiv informasjon.

7.2.2 Bedriftsintern informasjon

Dersom utvikler har bedt om at bedriftsintern informasjon ikke skal utleveres til oppdragsgiver, skal EVIT forvisse seg om at ETR ikke inneholder denne type informasjon før rapporten frigis. Normalt skjer det ved at EVIT utarbeider en kortversjon av ETR som deretter formidles til utvikler for nærmere vurderinger før frigivelse. Det bør fremgå av dokumentet om det er foreløpig eller endelig, og hvorvidt det er godkjent av sertifiseringsmyndigheten.

SERTIT kan nekte å gjennomføre en sertifisering, dersom utvikler ubegrunnet holder tilbake nødvendig bedriftsintern informasjon.

7.2.3 Vurdering og godkjenning av ETR

SERTIT gjennomgår ETR med underliggende dokumenter og undersøker om sikkerhetsevalueringen er gjennomført i henhold til de avtalte kriteriene, metodene og prosedyrene i ordningen, og om ETR gir et tilstrekkelig grunnlag for å utarbeide sertifiseringsrapporten (CR). SERTIT kan ved behov undersøke underliggende arbeidsrapporter.

For at ETR skal kunne godkjennes må alle merknader må være adressert og bevisene må være tilstrekkelige og konsistente iht. kravene i CCRA, SOGIS MRA og CC/CEM.

SERTIT utsteder så en bekreftelse på at sikkerhetsevalueringen er fullført og opplyser samtidig når CR er klar til offentliggjøring.

8 Sertifisering

Dette kapitlet gir en overordnet beskrivelse av selve sertifiseringsprosessen, samt hensikten med sertifiseringsrapporten (CR) og sertifikatet.

Sertifiseringsprosessen avsluttes med en formell bekreftelse av evalueringsresultatene, samt at evalueringskriteriene, metodene og prosedyrene er anvendt på korrekt måte. Prosessen for vedlikehold av sertifikatet er nærmere omtalt i kapittel 9.

8.1 Sertifiseringsprosessen

Sertifiseringsprosessen starter når det foreligger en godkjent ETR. SERTIT kan ved behov be EVIT om å få tilgang til særskilte tekniske bevis og andre resultater som understøtter konklusjonene i ETR. Foruten ETR utgjør øvrige dokumenter fra sikkerhetsevalueringen, observasjoner fra testingen og

resultater fra andre ettersynsaktiviteter viktig grunnlagsmateriale for sertifiseringen. Kapitlene 8.2 og 8.3 gir en nærmere beskrivelse av henholdsvis sertifiseringsrapporten og sertifikatet.

8.2 Sertifiseringsrapport

SERTIT skal dokumentere alle funn fra evalueringen i en sertifiseringsrapport. Sertifiseringsrapporten kan angi hvilket tillitsnivå (EAL) som er oppnådd, eller hvilke tillitskomponenter som inngår. Sertifiseringsrapporten kan anbefale passende mottiltak for å oppveie for eventuelle gjenstående sårbarheter. Hensikten med sertifiseringsrapporten er å bekrefte om TOE er i overensstemmelse med PP, cPP og/eller ST, samt å identifisere eventuelle sårbarheter som kan utnyttes. Sertifiseringsrapporten godtgjør derfor at sikkerhetsevalueringen er blitt gjennomført i henhold til gjeldende rammevilkår for ordningen, og at konklusjonene er konsistente og i tråd med de fremlagte bevis.

Sertifiseringsrapporten gir imidlertid ingen garanti for at alle feil og mangler er avdekket i TOE.

8.3 Sertifikat

Sertifikatet *"Certificate"* (C) utstedes normalt samtidig med CR, og tjener som en stadfesting av konklusjonene i CR. Leder for SERTIT gir endelig godkjenning av sertifikatet og sertifiseringsrapporten.

Utstedelsen av et sertifikat innebærer ikke noen form for anbefaling fra SERTIT vedrørende det spesifikke TOE.

Sertifikatet er kun gyldig for den versjonen, plattformen og de omgivelser TOE ble evaluert under.

Oppdragsgiver kan kun markedsføre et produkt som et sertifisert produkt på basis av et gyldig sertifikat. SERTIT kan kreve at oppdragsgiver fremlegger referansemateriell eller dokumentasjon som entydig viser korrekt versjon av TOE.

8.3.1 Rettigheter

SERTIT har kopirettighetene på sertifiseringsrapporten og sertifikatet. Reproduksjon og distribusjon kan tillates under forutsetning av at sertifiseringsrapporten kopieres i sin helhet.

8.3.2 Sertifiserte produkter

SERTIT vil regelmessig publisere en oversikt over hvilke produkter som er sertifisert under ordningen. Informasjon publiseres på internettsidene til SERTIT og CCRA.

8.3.3 Bruk av sertifikater

Følgende bestemmelser gjelder for bruk av sertifikatet:

- Sertifikatet må kun brukes i forbindelse med produktet som sertifikatet gjelder for,
- Sertifikatet må kun brukes til å dokumentere TOEs overensstemmelse med standardene som SERTIT baserer seg på,
- Sertifiseringen må ikke brukes på en feilaktig eller villedende måte som bringer eller kan bringe SERTIT eller sertifiseringsordningen i vanry,
- At sertifiseringen ikke benyttes i reklame eller markedsføring dersom sertifikatet er trukket tilbake eller ugyldig,
- Leverandøren er pliktig til å ha implementert registrering og behandling av klager vedrørende sertifiserte produkter, og gjort registreringene tilgjengelig for SERTIT.

Leverandøren er pliktig til å varsle SERTIT om alle endringer i forhold som var gjenstand for sikkerhetsevalueringen av det sertifiserte produktet.

For mer detaljerte bestemmelser om bruk av sertifikater, anbefales brukerne å leste dokumentet: *"Conditions for use of Certificate and Certification Mark"* [19].

8.3.4 Overvåkning av sertifikater

Overvåkning av sertifikater skjer primært ved gjennomgang av informasjon fra oppdragsgiver. Uttalelser om sertifiserte produkter i reklame, media eller oppdragsgivers nettsted eller andre forhold som kommer SERTIT til kunnskap, kan bli gjort gjenstand for nærmere undersøkelser.

Hensikten med overvåkningen er å se til at bruk av sertifikater skjer i tråd med bestemmelsene som angitt i kapittel 8.3.3 Bruk av sertifikater. Overvåkning av sertifikater skjer i tråd med definerte prosedyrer.

8.3.5 Sanksjoner ved misbruk av sertifikater

Ved misbruk av sertifikater kan SERTIT iverksette sanksjoner i henhold til ISO/IEC Guide 27 [11]. Håndtering av sanksjoner skjer i tråd med definerte prosedyrer. De to vanligste korrigerende tiltak er:

- Anmodning om tilbaketrekking av sertifikatet,
- Fjerne sertifiseringsmerket fra produktet.

9 Vedlikehold av sertifikatet

Et sertifikat er kun gyldig for en spesifikk versjon av TOE. De fleste TOE gjennomgår imidlertid endringer på et senere tidspunkt. Slike endringer ligger utenfor målet for sertifiseringen. Ved fremtidige endringer i TOE er det behov for at sluttbruker kan ha samme grad av tillit til den nye versjonen av TOE som i den opprinnelige sertifiserte versjonen. I CCRA og SOGIS MRA er det derfor etablert et rammeverk for vedlikehold av sertifikater, ref. [2] og [23]. SERTIT følger dette rammeverket i spørsmål som gjelder vedlikehold av sertifikater.

TOE kan derfor, under visse forutsetninger, være underlagt vedlikeholdsprogrammet. Rammeverket for vedlikeholdsprogrammet, kalt *"Assurance Continuity"*, kan lastes ned fra nettstedet til henholdsvis CCRA (www.commoncriteriaportal.org) og SOGIS (sogis.eu).

Ta kontakt med SERTIT for ytterligere informasjon om vedlikeholdsprogrammet.

Forkortelser

BI	Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (Beskyttelsesinstruksen)
CC	*Common Criteria*
CCRA	*Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security*
CEM	*Common Evaluation Methodology for Information Technology Security*
cPP	*Collaborative Protection Profile*
CR	*Certification Report,* (sertifiseringsrapport)
EAL	*Evaluation Assurance Level*, (tillitsnivå)
EOR	*Evaluation Observation Report*, (observasjonsrapport)
ETR	*Evaluation Technical Report*, (teknisk evalueringsrapport)
EVIT	Godkjent evalueringsfirma under den norske sertifiseringsordningen
NSM	Nasjonal sikkerhetsmyndighet
PP	*Protection Profile*, (kravspesifikasjon)
QP	*Qualified Participant*, (Kvalifisert sertifiseringsmyndighet)
SERTIT	Sertifiseringsmyndigheten for IT-sikkerhet
SOGIS MRA	*SOGIS Mutual Recognition Agreement*
ST	*Security Target*, (sikkerhetsobjekt, løsningsspesifikasjon)
TIN	*Task Initiation Notice,* (orientering om evalueringsoppdrag)
TOE	*Target of Evaluation*, (evalueringsobjekt)

Referanser

[1] Beskyttelsesinstruksen, *Instruks av 17. mars 1972 nr. 3352 for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter*.

[2] CCRA, (2012)*, Assurance Continuity: CCRA Requirements*, version 2.1, June 2012.

[3] CCRA, *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*, gjeldende versjon.

[4] CCRA, *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*, gjeldende versjon.

[5] CCRA, *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*, gjeldende versjon.

[6] CCRA, *Common Methodology for Information Technology Security Evaluation: Evaluation Methodology*, gjeldende versjon.

[7] CCRA, (2014), *"Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security"*, 2 July 2014.

[8] Forskrift om offentlige arkiv, *Forskrift av 15. desember 2017 nr. 2105 om offentlige arkiv*.

[9] Forskrift om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver, *Forskrift av 19. desember 2017 nr. 2286 om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver (riksarkivarens forskrift)*.

[10] Forvaltningsloven*, Lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker*, Hentet fra: https://lovdata.no/dokument/NL/lov/1967-02-10

[11] ISO (1982), "*Guidelines for corrective action to be taken by a certification body in the event of misuse of its mark of conformity",* ISO/IEC Guide 27:1983, International Organization for Standardization.

[12] ISO, *Information technology – Security techniques – Evaluation criteria for IT security*, ISO/IEC 15408, gjeldende versjon, International Organization for Standardization.

[13] ISO (2009), *Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets*, ISO/IEC TR 15446:2009, gjeldende versjon, International Organization for Standardization,

[14] ISO, *Information technology – Security techniques – Methodology for IT security evaluation*, ISO/IEC 18045, gjeldende versjon, International Organization for Standardization.

[15] Personopplysningsloven (2018), *Lov av 15. juni 2018 nr. 38 om behandling av personopplysninger,* Hentet fra https://lovdata.no/dokument/NL/lov/2018-06-15-38.

[16] Rådet for IT-sikkerhet, (1997), *Sertifisering av IT-sikkerhet i produkter, systemer og organisasjoner (sluttrapport)*, 13. november 1997.

[17] SERTIT (2020), *Krav til evalueringsfirma – kvalifiseringskrav til evalueringsfirma under den offentlige sertifiseringsordningen for IT-sikkerhet*, SD 003, v. 4.2, 06.04.2020, SERTIT.

[18] SERTIT, *Application for certification* ST 027E, v. 2.5, SERTIT.

[19] SERTIT (2018), *Conditions for use of Certificate and Certification Mark*, SD 030E, v 3.1, SERTIT.

[20] SERTIT (2017), *Driftsavtale,* SD 006, v. 2.0, SERTIT.

[21] SERTIT (2017), *Mandat for SERTIT*, v. 1.0, 29.11.2017, SERTIT.

[22] Sikkerhetsloven (2018), *Lov om nasjonal sikkerhet (sikkerhetsloven), Lov av 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven)*, Hentet fra https:// lovdata.no/dokument/NL/lov/2018-06-01-24.

[23] SOGIS (2019), *Assurance Continuity*, v. 1.0, November 2019, Joint Interpretation Library, SOGIS, Hentet fra: https://www.sogis.eu/uk/detail_operation_en.html.

[24] SOGIS MRA, (2010), *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, Version 3.0, January 8th 2010.

[25] Standard Norge (2017), *Generelle krav til prøvings- og kalibreringslaboratoriers kompetanse* (ISO/IEC 17025:2017), November 2017, Standard Norge.

[26] Standard Norge (2012), *Samsvarsvurdering Krav til sertifiseringsorganer for produkter, prosesser og tjenester* (ISO/IEC 17065:2012), September 2012, Standard Norge.

Vedlegg A: Historikk

En utredningsgruppe under Rådet for IT-sikkerhet utarbeidet høsten 1997 en rapport [16] som blant annet anbefalte å opprette en ordning for sertifisering av IT-sikkerhet i produkter og systemer. Regjeringen besluttet deretter å opprette ordningen i henhold til anbefalingen. Stortinget bevilget på bakgrunn av St. prp. nr. 1 (1998-99) for Nærings- og handelsdepartementet (NHD) midler til daværende Forsvarets overkommando/Sikkerhetsstaben (FO/S) til etablering og drift av SERTIT. SERTIT har vært en del av Nasjonal sikkerhetsmyndighet (NSM) siden 1.1.2003.