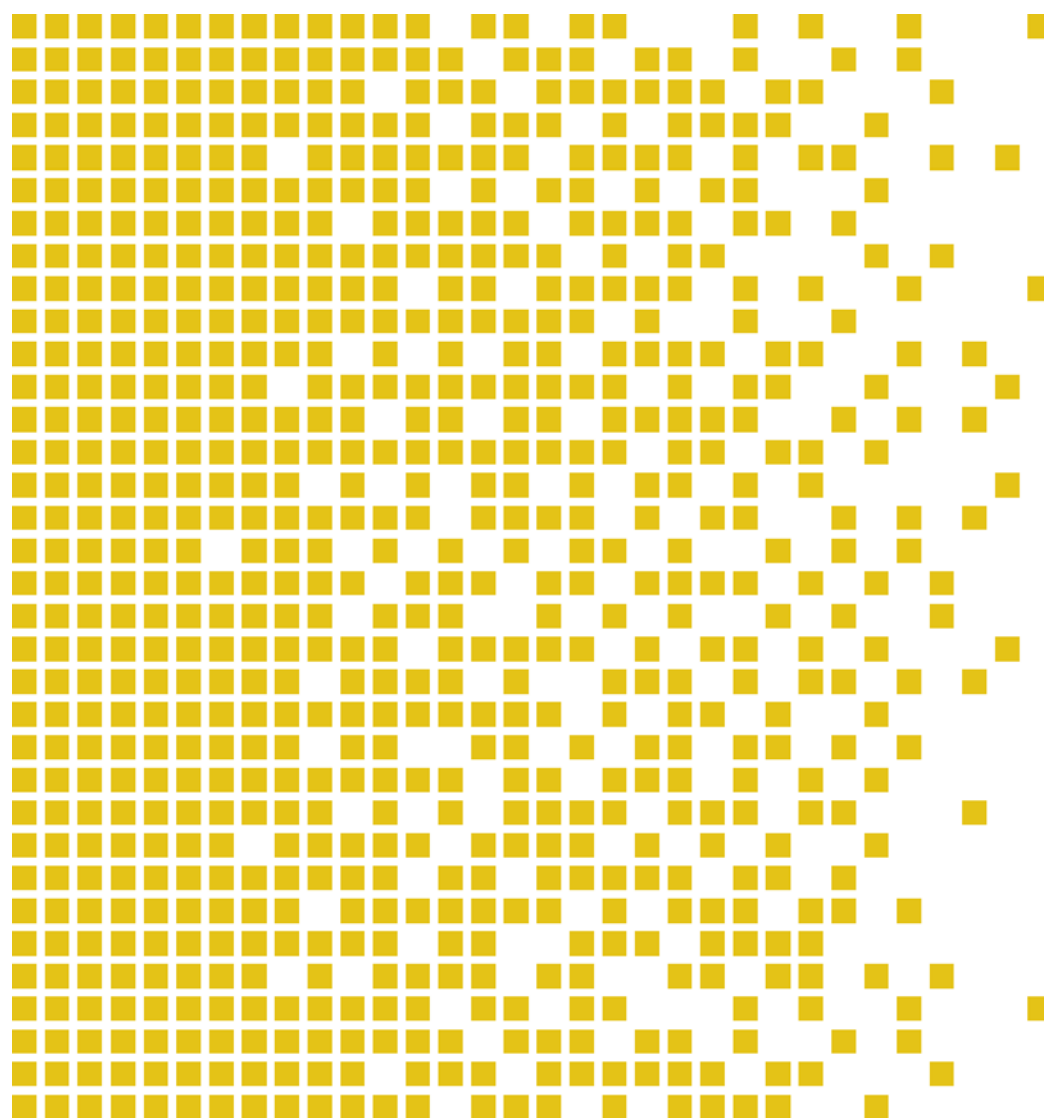


Om sertifiseringsordningen

IT-sikkerhet i produkter og systemer



PUBLIKASJON SD 001 VERSJON 8.0 DATO: 18.02.2010

Dokumenthistorikk

Dokument tittel	Om sertifiseringsordningen, IT-sikkerhet i produkter og systemer, Sd 001, Versjon 8.0, 18. februar 2010.
-----------------	--

Dato	Beskrivelse
18. februar 2010	Publisert versjon 8.0
8. februar 2008	Publisert versjon 7.0
2. juli 2007	Publisert versjon 6.0
10. mars 2005	Publisert versjon, 5.0
16. september 2004	Publisert versjon, 4.0.
1. november 2002	Publisert versjon, 3.0.
23. august 2002	Publisert versjon, 2.3C.

<p style="text-align: center;"><u>Siste versjon kontrollert</u></p> <p>Kolsås, 18.02.2010</p> <p style="text-align: center;"><i>9/3-2010</i></p> <hr/> <p style="text-align: center;"><i>Anne H. Røge</i></p> <hr/> <p style="text-align: center;">Ansvarlig for kvalitetskontroll</p>	<p style="text-align: center;"><u>Siste versjon godkjent</u></p> <p>Kolsås, 18.02.2010</p> <p style="text-align: center;"><i>Kjell W. Bergan</i></p> <hr/> <p style="text-align: center;">Kjell W. Bergan</p> <hr/> <p style="text-align: center;">Leder for SERTIT</p>
--	---



Innhold

1	Oversikt over sertifiseringsordningen	7
1.1	Bakgrunn	7
1.2	Historikk	7
1.3	IT-sikkerhet	7
1.4	Utfordringer	8
1.5	Formål	8
1.6	Rammer	9
1.7	Målgrupper	9
1.8	Sikkerhetsevaluering og sertifisering	10
2	Prinsipper for sertifiseringsordningen	10
3	Organisering og ansvar	11
3.1	Nasjonal sikkerhetsmyndighet	11
3.2	SERTIT	11
3.3	Fagråd	12
3.4	Evalueringsfirma (EVIT)	12
3.5	Eksterne parter	12
3.5.1	Oppdragsgiver	12
3.5.2	Utvikler	12
4	Generelle bestemmelser	13
4.1	Gjennomføring av sikkerhetsevaluering	13
4.2	Rammevilkår for evalueringsvirksomhet	13
4.3	Regler for publisering av informasjon	13
4.4	Klager, tvister og tilbakemeldinger	14
5	Finansiering av sertifiseringsordningen	14
6	Forberedelser til sikkerhetsevaluering	14
6.1	Kravspesifikasjon	15
6.2	Sikkerhetsobjekt	15
6.3	Leveranser	15
6.3.1	Opphavsrett og andre rettigheter	16
6.4	Varsling av oppdrag og fremdriftsplan for sikkerhetsevalueringen	16
6.5	Søknad om sertifisering	16
6.6	Avklaringer og tilsagn	16
6.7	Godkjenning av sertifiseringsoppdrag	17
6.8	Bruk av konsulenter	17
6.8.1	Kontraktsmessige forhold	18
7	Sikkerhetsevaluering	18
7.1	Mål	19
7.2	Gjennomføring	19
7.2.1	Observasjonsrapporter og dagbok	19
7.2.2	Interaksjon	19
7.2.3	Inspeksjon	20
7.3	Teknisk evalueringsrapport	20

7.3.1	Beskyttelse av informasjon og beskyttelsesmerking av ETR	20
7.3.2	Bedriftsintern informasjon	21
7.3.3	Vurdering og godkjenning av ETR	21
8	Sertifisering	21
8.1	Sertifiseringsprosessen	21
8.2	Sertifiseringsrapport	22
8.3	Sertifikat	22
8.3.1	Rettigheter	22
8.3.2	Sertifiserte produkter	22
8.3.3	Bruk av sertifikater	22
8.3.4	Overvåkning av sertifikater	23
8.3.5	Sanksjoner ved misbruk av sertifikater	23
9	Vedlikehold av sertifikatet	24
10	Forkortelser	24
11	Referanser	24
	Vedlegg A: Organisering av sertifiseringsordningen	26
	Vedlegg B: Organisasjonskart for SERTIT – funksjoner og roller	27
	Vedlegg C: Mandat for SERTIT	28

1 Oversikt over sertifiseringsordningen

Dette dokumentet beskriver den offentlige ordningen for sertifisering av IT-sikkerhet i produkter og systemer. Det er sertifiseringsmyndigheten for IT sikkerhet (SERTIT) som utformer rammevilkår og regler for sertifisering av IT-sikkerhet i produkter og systemer i Norge. Det er også SERTIT som forestår sertifisering av IT-produkter og systemer.

Dette dokumentet gir en oversikt over sertifiseringsordningen, policy, organisering og ansvar, finansiering, forberedelser og gjennomføring av sikkerhetsevaluering og til slutt sertifisering og vedlikehold av sertifikatet.

SERTIT tar alle forbehold om fremtidige endringer i dokumentet.

Alle henvendelser vedrørende dette dokumentet eller kommentarer til innholdet, skal rettes til: SERTIT.

1.1 Bakgrunn

I lys av den raske IT-utviklingen, og tiltakende bruk av IT-systemer for informasjonsbehandling innenfor både offentlig- og privat sektor samt på privat basis, har behovet for en uavhengig sikkerhetsmessig vurdering økt tilsvarende.

1.2 Historikk

En utredningsgruppe under Rådet for IT-sikkerhet utarbeidet høsten 1997 en rapport [20] som blant annet anbefalte å opprette en ordning for sertifisering av IT-sikkerhet i produkter og systemer. Regjeringen besluttet å opprette ordningen iht. 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. FO/S er fra 1.1.2003 blitt til direktoratet Nasjonal sikkerhetsmyndighet (NSM) under Forsvarsdepartementet (FD).

1.3 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 tre sentrale begreper; tilgjengelighet, integritet og konfidensialitet.

- Tilgjengelighet (Sikre at informasjon og dataressurser er tilgjengelig for autoriserte brukere til rett tid og i rett form),
- Integritet (Sikre at informasjonen er korrekt og ikke blir endret eller ødelagt av uvedkommende),
- Konfidensialitet (Sikre at informasjonen ikke blir kjent for uvedkommende).

IT-sikkerhet er med andre ord tiltak og virkemidler for å beskytte informasjon som lagres, behandles og kommuniseres i IT-systemer. Det er denne forståelsen av IT-sikkerhet som gjelder i dette dokumentet.

1.4 utfordringer

Å foreta et valg av IT-systemer som skal oppfylle bestemte sikkerhetskrav fordrer inngående kjennskap til løsningenes styrker og svakheter, og ikke minst tilgang til informasjon om dette. Mangel på informasjon eller misvisende informasjon kan blant annet føre til feilinvesteringer eller for lav IT-sikkerhet.

Det foreligger minst tre muligheter i vurderingen av IT-sikkerhet:

- Det første alternativet er å stole på leverandørens forsikringer om IT-produktets eller systemets beskaffenhet og sikkerhet. Det viser seg imidlertid ofte ved nærmere ettersyn og utprøving av løsningene, at det fortsatt finnes uløste sikkerhetsmessige problemer og at IT-produktet eller systemet også inneholder feil og mangler. Leverandøren svarer gjerne med å tilby feilretting eller oppgradering, men i mellomtiden har løsningen vært operativ og informasjonen uten den beskyttelse som var forutsatt,
- Det andre alternativet er å gjennomføre egne tester og vurderinger, men slike tester er tidkrevende og forutsetter særskilt kompetanse. I et samfunnsmessig perspektiv er det dessuten lite formålstjenlig at hver enkelt skal bruke ressurser på kartlegging av om et IT-produkt eller system tilfredsstillende gir funksjonelle sikkerhetskrav og krav til tillit,
- Det tredje alternativet er å la en uavhengig tredjepart med den nødvendige kompetanse gjennomføre vurderingene. Vurderingene gjennomføres etter internasjonalt anerkjente kriterier og metoder som sikrer at alle trinn i vurderingsprosessen blir gjennomført på korrekt måte. I et samfunnsmessig perspektiv er dette mer rasjonelt for å sikre at IT-produktet eller systemet tilfredsstillende gir krav som er satt, ved at det gjennomføres en samlet vurdering samtidig som det forenkler anskaffelsesprosessen for kundene.

Hensikten med sertifiseringsordningen er å tilby tjenester som bygger opp under det tredje alternativet, og fortsettelsen av dette dokumentet handler derfor utelukkende om dette alternativet.

1.5 Formål

Formålet med ordningen er blant annet å dekke myndighetenes og industriens behov for en kostnadseffektiv og rasjonell sikkerhetsmessig evaluering og sertifisering av IT-produkter og systemer.

Norge har derfor i et internasjonalt arrangement, se kapitlene 1.6, 1.8 og referanse [5], forpliktet seg til å anerkjenne sertifikater som er utstedt av kvalifiserte sertifiseringsmyndigheter. IT-produkter og systemer skal sikkerhetsevalueres og sertifiseres i henhold til de internasjonale evalueringskriteriene Common Criteria (CC) [1], [2] og [3], svarende til ISO 15408 og metodikken Common Evaluation Methodology (CEM) [4] og [6].

1.6 Rammer

Sertifiseringsordningen under SERTIT bygger på følgende internasjonale arrangement:

- **Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security (CCRA) [5].**

SERTIT har i tillegg valgt å ta med følgende nasjonale dokumenter som dermed danner føringen for de involverte parter under sertifiseringsordningen:

- **Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) [15],**
- **Forskrift om informasjonssikkerhet [7],**
- **Forskrift om sikkerhetsgraderte anskaffelser [8],**
- **Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (Beskyttelsesinstruksen) [11],**
- **Lov om behandling av personopplysninger (personopplysningsloven) [14].**

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

1.7 Målgrupper

Ettersom kravene og bevisstgjøringen til IT-sikkerhet i produkter- og systemer er sterkt økende i samfunnet, er også nedslagsfeltet for ordningen voksende og målgruppen er således bredt sammensatt. Følgende målgrupper er sentrale for ordningen:

- **De som skal utvikle/produsere,**
- **De som skal tilby/selge,**
- **De som skal kjøpe/anskaffe.**

I tillegg vil de som skal godkjenne IT-systemer dra nytte av at produkter er sertifisert av en uholdet tredjepart. Dette gjelder både aktører som er underlagt formelle sikkerhetsbestemmelser for informasjonssikkerhet og aktører som faller utenfor sikkerhetsreglene. Dette omfatter sektorer som er ansvarlig for samfunns- og virksomhetskritiske systemer.

1.8 Sikkerhetsevaluering og sertifisering

For alle kategorier IT-brukere, så vel i offentlig som privat sektor eller på privat basis, er det viktig å få et mål på hvilke krav systemet tilfredsstillter. I tillegg er det også av betydning å kunne ha tillit til at IT-produktet eller systemet har gjennomgått en uhildet vurdering av en nøytral faginstans. Dette er oppnådd gjennom etableringen av sertifiseringsordningen.

Norge er forpliktet seg til å gjennomføre sikkerhetsevaluering og sertifisering i henhold til internasjonalt anerkjente standarder og metodikker slik disse er definert i CCRA [5].

CCRA inneholder to sentrale elementer:

- Alle som deltar er forpliktet til å godkjenne sertifikater som er utstedt under CCRA,
- Godkjenne etablering av kvalifiserte sertifiseringsmyndigheter, "*Qualified Participants (QP)*".

I henhold til dette anerkjenner Norge alle sertifikater som er utstedt under CCRA. Norge har status som QP, noe som innebærer at sertifikatene anerkjennes internasjonalt.

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

2 Prinsipper for sertifiseringsordningen

Følgende prinsipper er lagt til grunn for sertifiseringsordningen:

- SERTIT er upartisk og uhildet og har ingen andre aktiviteter ved siden av de daglige gjøremålene i sertifiseringsordningen,
- Bruk av sertifiseringsordningen er basert på frivillighet,
- Grunnlaget for sertifiseringen er en avsluttet evaluering i tråd med ordningens rammevilkår,
- Sikkerhetsevalueringen gjennomføres av godkjente evalueringsfirma som driver etter vanlige forretningsmessige prinsipper,
- SERTIT godkjenner evalueringsfirma og fører tilsyn med virksomheten,
- Ordningen er åpen og tilgjengelig for alle som ønsker å søke om sertifisering,
- SERTIT avgjør om produktet/systemet er egnet for sertifisering.

Alle som er berørt av ordningen og har synspunkter om SERTIT, sertifiseringsordningen, sertifisering eller andre forhold har anledning til å gi tilbakemeldinger og innspill.

3 Organisering og ansvar

Den offentlige sertifiseringsordningen for IT-sikkerhet forvaltes av SERTIT.

SERTIT er en del av Nasjonal sikkerhetsmyndighet (NSM). Det er etablert et fagråd for SERTIT. Sertifiseringsordningen er illustrert i vedlegg¹.

Partenes hovedoppgaver og ansvarsområder er nærmere beskrevet nedenfor og i tilhørende vedlegg.

3.1 Nasjonal sikkerhetsmyndighet

NSM koordinerer de forebyggende sikkerhetstiltak og kontrollerer sikkerhetstilstanden i Norge. NSMs ansvarsområde er dels gitt gjennom lov om forebyggende sikkerhetstjeneste og dels gjennom de årlige tildelings- og iverksettelsesbrevene.

3.2 SERTIT

SERTIT er den offentlige sertifiseringsmyndigheten for IT-sikkerhet.

SERTITs hovedoppgave som offentlig sertifiseringsmyndighet for IT-sikkerhet er primært å utstede sertifikater og sertifiseringsrapporter. I tillegg er SERTIT ansvarlig for å utforme rammevilkår og regler for ordningen, og påse at reglene følges av alle parter. SERTIT fører også tilsyn med hele evalueringsprosessen som utgjør grunnlaget for å kunne utføre sertifisering. SERTIT er dessuten godkjenningmyndighet ved etablering av kommersielle evalueringsfirma under sertifiseringsordningen. SERTITs mandat er gitt i vedlegg².

For å ivareta oppgavene i SERTIT på en hensiktsmessig måte, herunder oppfylle de formelle kravene [4], [5], [16] og [17], 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 gjennomføres under tilsyn av en prosjektansvarlig som også er ansvarlig for utforming av sertifiseringsrapport og sertifikat. Personell til denne rolles pekes ut i de enkelte prosjektene i tråd med gjeldende prosedyrer angitt i kvalitetssystemet. SERTIT er ansvarlig for at oppgaver med kvalitetssystemet, økonomi/administrasjon, kommunikasjon og marked blir tatt hånd om på en tilfredsstillende måte.

Organisasjonskart for SERTIT er gitt i vedlegg³ og viser en grafisk fremstilling av SERTIT og hvilke funksjoner som håndteres i virksomheten.

¹ Vedlegg A: Organisering av sertifiseringsordningen

² Vedlegg C: Mandat for SERTIT.

³ Vedlegg B: Organisasjonskart for SERTIT – funksjoner og roller.

3.3 Fagråd

Det er etablert et fagråd for SERTIT som foruten å gi faglige råd skal bidra til nødvendig dialog mellom sertifiseringsmyndigheten og interessentene for ordningen.

3.4 Evalueringsfirma (EVIT)

Evalueringsfirma som utfører oppdrag for sertifiseringsordningen er underlagt SERTITs myndighetskontroll. Dette betyr blant annet at SERTIT er ansvarlig for å godkjenne evalueringsvirksomheten, og senere foreta kontroller av firmaet og alle evalueringsaktiviteter. Evalueringsvirksomheten er regulert gjennom bestemmelsene i CCRA [5] og nasjonale rammevilkår fastlagt av SERTIT.

Evalueringsfirmaene utfører sikkerhetsevaluering av IT-produkter og systemer på et forretningsmessig grunnlag i henhold til internasjonale standarder [1], [2], [3], [4] og [16]. EVIT gjennomfører sikkerhetsevaluering i henhold til definerte prosedyrer som er nedfelt i en egen kvalitetshåndbok.

Informasjon om godkjente evalueringsfirma kan finnes i vedlegg A. En fullstendig oppdatert oversikt over godkjente evalueringsfirma finnes på www.sertit.no.

3.5 Eksterne parter

I sertifiseringsprosessen er det flere eksterne parter. Det vanligste er å skille mellom oppdragsgiver og utvikler, men det kan også være flere aktører involvert i prosessen. Nedenfor følger en nærmere beskrivelse av aktørene og noen retningslinjer i sertifiseringsprosessen.

3.5.1 Oppdragsgiver

Med oppdragsgiver menes en organisasjon eller person som anmoder om en sertifisering for et bestemt IT-produkt eller system. En oppdragsgiver kan derfor ha ulik tilknytning til IT-produktet eller systemet som skal sertifiseres.

En oppdragsgiver kan være en leverandør, anskaffer, agent som handler på oppdrag for en anskaffer, systemutvikler eller et konsortium som representerer flere utviklere eller leverandører.

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

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

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

3.5.2 Utvikler

Med utvikler menes den bedrift som produserer IT-produktet eller systemet 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 eller systemet 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 6.8.1.

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 nærmere detaljer vises til publikasjonen Sd 003 [18].

4.1 Gjennomføring av sikkerhetsevaluering

Alle oppdrag for sikkerhetsevaluering av IT-produkter og systemer under sertifiseringsordningen krever formell forhåndsgodkjenning av SERTIT.

Sertifiseringsordningen bygger på tillit og nøytral faglig vurdering.

SERTIT fører tilsyn 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 [18].

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

SERTIT er 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 SERTIT. 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 Finansiering av sertifiseringsordningen

Forsvarsdepartementet (FD) er budsjettansvarlig departement og bevilger midler til SERTIT gjennom budsjettet til Nasjonal sikkerhetsmyndighet.

Bevilgningen til SERTIT dekker sertifiseringsmyndighetens årlige driftsutgifter.

6 Forberedelser til sikkerhetsevaluering

Dette kapitlet omtaler utgangspunktet for å gjennomføre sertifisering, og beskriver nærmere de forberedende fasene av sertifiseringsprosessen.

Utgangspunktet for å sette i verk en sertifiseringsprosess er normalt ett eller flere av følgende forhold:

- leverandør ønsker å styrke sin markedsmessige posisjon,
- krav til systemutvikler om å tilfredsstille gitte betingelser i en bestemt kontrakt,
- anskaffer av et produkt eller system må følge bedriftens egne sikkerhetskrav, bransjekrav eller sikkerhetskrav gitt i medhold av lov eller forskrift.

Målsettingen med den forberedende fasen er å undersøke om evalueringsobjektet, "*Target of Evaluation (TOE)*", er klart definert og om objektet er hensiktsmessig å sertifisere.

Dette omfatter i tillegg til TOE normalt følgende forhold: Kravspesifikasjon, utforming og kvalitetssikring av sikkerhetsobjektet, "*Security Target (ST)*", identifisere hvilke leveranser som er nødvendig for gjennomføring av evalueringen,

formell varsling av oppdraget og utforming av fremdriftsplaner, søknad om sertifisering, avklare hensikten med og målet for evalueringen.

Nedenfor behandles de enkelte trinn i forberedelsene nærmere.

6.1 Kravspesifikasjon

"*Protection Profile (PP)*" er et generisk sett av funksjonelle sikkerhetskrav og krav til tillitsnivå for en bestemt type/gruppe TOE og som er utviklet for å definere virksomhetens sikkerhetskrav. Sagt på en annen måte kan vi kalle PP for en kravspesifikasjon for sikkerhet. ST kan bestå av hele eller deler av en eller flere PP. PP kan sikkerhetsevalueres og sertifiseres i henhold til kravene i CC.

6.2 Sikkerhetsobjekt

Med ST menes både en spesifikasjon av de sikkerhetsfunksjoner TOE skal vurderes opp mot og en beskrivelse av det miljøet TOE skal operere i. ST er med andre ord en løsningsspesifikasjon.

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

CC angir krav til form og innhold av ST.

Oppdragsgiver kan benytte ekstern bistand til utforming av ST.

6.3 Leveranser

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

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

Leveransene er helt nødvendige for at sikkerhetsevalueringen skal kunne gjennomføres. EVIT er ansvarlig for å dokumentere leveransene i en egen liste.

6.3.1 Opphavsrett og andre rettigheter

Det er normalt utvikleren som har opphavsrett til informasjon om TOE, og det er ingen automatikk i at oppdragsgiver har tilgang til denne typen informasjonen. Dette bør derfor reguleres i en særskilt avtale mellom partene, se også kapittel 6.8.1 Kontraktsmessige forhold.

6.4 Varsling av oppdrag og fremdriftsplan for sikkerhetsevalueringen

EVIT er pålagt av SERTIT å varsle om nytt oppdrag, "*Task Initiation Notice (TIN)*", og be om aksept til å gjennomføre sikkerhetsevaluering under ordningen. Dette skjer normalt etter forutgående undersøkelser av grunnlaget for sikkerhetsevalueringen. Prosedyrene for varsling av oppdrag er definert nærmere i egne retningslinjer for EVIT.

Det skal også utformes en fremdriftsplan for sikkerhetsevalueringen som føres på blanketten "*Evaluation Work Plan (EWP)*". EWP skal ha et tilstrekkelig detaljeringsnivå som omfatter alle evalueringsaktiviteter. Prosedyrene for utfylling av EWP er definert nærmere i egne retningslinjer for EVIT.

Begge dokumentene skal fremsendes samlet til SERTIT for nærmere vurdering, og deretter avholdes normalt et møte mellom partene.

På bakgrunn av den formelle henvendelsen fra EVIT peker leder for SERTIT ut bemyndiget personell til å føre tilsyn med det videre arbeidet.

6.5 Søknad om sertifisering

Oppdragsgiver er ansvarlig for å fremme søknad om sertifisering til SERTIT. Det er utformet et eget søknadsskjema [19] som kan lastes ned fra SERTITs websider og som skal benyttes ved alle formelle henvendelser om sertifisering.

Søknadsskjemaet inneholder veiledning for utfylling og gir nærmere regler for tildeling og bruk av sertifikat. Søknaden forplikter oppdragsgiver til å følge alle 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 søknaden med nødvendige vedlegg fremsendes til SERTIT samtidig med oversendelsen av TIN og EWP fra EVIT siden søknaden ikke kan behandles før TIN og EWP foreligger.

6.6 Avklaringer og tilsagn

Før det inngås bindende avtaler om sikkerhetsevaluering og påfølgende sertifisering er det viktig at oppdragsgiver undersøker saken med SERTIT, herunder om det foreslåtte TOE prinsipielt kan sertifiseres under ordningen. I praksis skjer dette normalt ved at oppdragsgiver, EVIT og SERTIT behandler saken i et startmøte. Startmøtet finner normalt sted etter at partene har vurdert foreliggende

dokumentasjon, forutsatt at det er stor sannsynlighet for å kunne gjennomføre sertifisering.

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

6.7 Godkjenning av sertifiseringsoppdrag

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

- Sertifisering må være hensiktsmessig,
- De formelle kravene for sertifisering må være oppfylt,
- Sikkerhetsevaluering og sertifisering må kunne gjennomføres på en uhildet måte,
- Sikkerhetsevalueringen og sertifiseringsordningen må være i samsvar med internasjonale og nasjonale bestemmelser,
- Det må fremgå av EWP 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,
- Eventuelle andre forhold som tilsier at sertifisering ikke kan gjennomføres.

Godkjenningen kan gis muntlig i møte med partene, men må senere bekreftes gjennom en formell godkjenning. Det skal bekreftes at både ST, TOE, leveransene og EWP kan aksepteres som en del av den foreslåtte sikkerhetsevalueringen under sertifiseringsordningen. Godkjenningen blir sendt til alle involverte parter.

6.8 Bruk av konsulenter

Bruk av konsulentbistand ved forberedelser til en sikkerhetsevaluering er ikke underlagt SERTITs kontroll, og er derfor gjenstand for forhandlinger mellom oppdragsgiver og EVIT eller øvrige konsulenter. Bruk av konsulenter til utvikling eller forberedelser til evaluering er normalt uproblematisk så lenge firmaet kan vise at kravene om uhildethet er tilfredsstillt. 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 hindrer 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 skal EVIT kontakte SERTIT for å få bekreftet at det ikke er innvendinger mot å gjennomføre arbeidet slik som angitt.

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. EVIT er pålagt å underrette SERTIT om all konsulentvirksomhet som er relatert til evalueringsoppdrag.

6.8.1 Kontraktsmessige forhold

Oppdragsgiver oppfordres til å innhente tilbud fra flere evalueringsinstanser i samband med forberedelser eller gjennomføring av sikkerhetsevaluering.

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 påbegynnes. Det er opp til partene å definere detaljene i avtalen nærmere, men følgende forhold bør være omfattet:

Å angi behovet for å få tilgang til tidligere evalueringsrapporter som er ønsket fra oppdragsgiver,

Avtalen bør håndtere alle forhold knyttet til Leveranser som angitt i kapittel 6.3. Dette omfatter blant annet tidsplaner for å fremskaffe leveransene, innsynsrett og krav til oppbevaring. Eiendomsrett til informasjon bør være avklart før oppdraget starter.

Alle forhold som vedrører bedriftssensitiv informasjon bør være håndtert i avtalen.

SERTIT anbefaler at avtalen regulerer alle forhold ved bruk av konsulenter, dette for å sikre at nødvendig grad av uhildethet opprettholdes. Dette gjelder også i de tilfeller det gjennomføres konsulentoppdrag utenfor rammen av sertifiseringsordningen, men som er knyttet til produkter/systemer som senere blir gjenstand for sikkerhetsevaluering og sertifisering.

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.

Oppdragsgiver kan ikke uten videre trekke seg fra et påbegynt sertifiseringsoppdrag. SERTIT krever generelt at EVIT har regulert alle forhold vedrørende et eventuelt kontraktsbrudd i en egen avtale for hvert enkelt oppdrag. Oppdrag uten fremdrift i 6 måneder kan termineres.

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 Mål

Med sikkerhetsevaluering menes i denne sammenheng å bedømme om et IT-produkt eller -system oppfyller kravene i ST. Dette omfatter slik som å bedømme en detaljert evaluering av TOE for å fastslå hvor godt den oppfyller ST samt å identifisere mulige feil og mangler. Målet er å gjøre EVIT i stand til å utarbeide en uhildet rapport som fastslår om TOE tilfredsstillende ST eller ikke.

7.2 Gjennomføring

Den tekniske sikkerhetsevalueringen av TOE og leveransene gjennomføres i henhold til godkjent EWP. Sikkerhetsevalueringen utføres i henhold til gjeldende internasjonale bestemmelser gjennom CCRA, CC, CEM og øvrige nasjonale rammevilkår fastsatt av SERTIT.

Eventuelle endringer i EWP skal vurderes og godkjennes av SERTIT, dette blant annet for å sikre at det foreslåtte arbeidet er tilstrekkelig, at planene er realistiske og at nødvendige ressurser er tilgjengelig. For øvrig vises til bestemmelsene i kap 6.8.1 Kontraktsmessige forhold, siste setning.

Både SERTIT og EVIT 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.

7.2.1 Observasjonsrapporter og dagbok

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 korrigerende påviste feil og mangler samt en tidsplan for eventuelle utbedringer. Utbedringene kan kreve justeringer i leveransene og kan ha konsekvenser for EWP. Synspunkter fra SERTIT fremmes normalt gjennom en særskilt blankett for merknader. EOR og merknader til EOR er saksdokumenter til fremdriftsmøtene, se kapittel 7.2.2. Prosessen går normalt i iterasjoner mellom partene helt til EOR er løst. I de tilfellene det ikke er mulig å løse EOR vises til siste avsnitt i kapittel 7.2.2 Interaksjon.

I tillegg til EOR skal EVIT løpende dokumentere aktivitetene og resultatene fra sikkerhetsevalueringen i en egen logg for hvert enkelt evalueringssoppgave. SERTIT kan undersøke loggen ved behov.

7.2.2 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 EWP.

EVIT har normalt behov for å kommunisere direkte med utvikler om TOE, leveransene eller andre forhold. Det forsettes 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 møterefateret.

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. Oppdragsgiver kan deretter velge å:

- avbryte sikkerhetsevalueringen,
- fortsette sikkerhetsevalueringen og akseptere problemene og konsekvensene for evalueringen, for eksempel gjennom et lavere tillitsnivå (EAL),
- endre evalueringsplanen og i samråd med SERTIT instruere utvikler om å foreta de nødvendige endringer i TOE.

Oppdragsgiver må bekrefte skriftlig hvilket alternativ som velges.

7.2.3 Inspeksjon

SERTIT kan som ett ledd i tilsynsvirksomheten foreta nødvendige inspeksjoner for å sikre at rammevilkårene for sikkerhetsevalueringen blir fulgt. SERTIT kan være tilstede under testing.

SERTIT forbeholder seg retten til å bevitne sikkerhetsevalueringen på nærmere angitte premisser mellom partene.

7.3 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, annekst I 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.

7.3.1 Beskyttelse av informasjon og beskyttelsesmerking av ETR

Det må klart fremgå av rapporten dersom innholdet er å anse som bedriftsintern 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 bedriftsintern informasjon.

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. SERTIT og EVIT skal sørge for at oppdragsgiver ikke får tilgang til denne type informasjon. EVIT er ansvarlig for at omfanget av denne type informasjon er klart definert og at reglene for beskyttelse av slik informasjon følges.

7.3.2 Bedriftsintern informasjon

Dersom utvikler har bedt om at bedriftsintern informasjon ikke skal utleveres til oppdragsgiver, skal EVIT forvise 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 oppdragsgiver for nærmere vurderinger. 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

7.3.3 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 at ETR gir et tilstrekkelig grunnlag for å utarbeide sertifiseringsrapporten (CR).

For at ETR skal kunne godkjennes må alle merknader må være adressert og bevisene må være tilstrekkelige og konsistente iht kravene i CCRA 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 evalueringresultatene, samt at evalueringskriteriene, metodene og prosedyrene er anvendt på korrekt måte. Planer om å tilby 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 resultater for å understøtte konklusjonene som er angitt i ETR. Øvrige dokumenter fra sikkerhetsevalueringen, observasjoner fra testingen og resultater fra andre tilsynsaktiviteter utgjør samtidig 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. Hensikten med sertifiseringsrapporten er å bekrefte om TOE er i overensstemmelse med ST, samt å identifisere eventuelle sårbarheter som kan utnyttes. Sertifiseringsrapporten bekrefter hvilket tillitsnivå som er oppnådd. Sertifiseringsrapporten kan anbefale passende mottiltak for å oppveie for eventuelle sårbarheter. Sertifiseringsrapporten bekrefter at sikkerhetsevalueringen er blitt gjennomført i henhold til rammevilkårene 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. Sannsynligheten for gjenstående feil eller mangler er imidlertid mindre desto høyere tillitsnivå (EAL) som ligger til grunn for evalueringen.

8.3 Sertifikat

Når CR er ferdigstilt, kan det utstedes et sertifikat som samtidig er en aksept for punktene nevnt over. Sertifiseringsrapporten skal vedlegges sertifikatet. 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 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 SERTITs nettsider. Henvendelser om sertifisering, sertifiseringsordningen eller andre forhold kan rettes til SERTIT.

8.3.3 Bruk av sertifikater

Følgende bestemmelser gjelder for bruk av sertifikatet:

- Sertifikatet må kun brukes i forbindelse med produktet/systemet som sertifikatet gjelder for,
- Sertifikatet må kun brukes til å dokumentere produktets/systemets 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 ved opphevelse eller tilbaketrekking av sertifikatet,
- 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

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 overvåkingen 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 [12]. 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 sertifisering. Det er derfor behov for å kunne tilby et opplegg for å håndtere fremtidige endringer i TOE, slik at en sluttbruker kan ha samme grad av tillit til den nye versjonen av TOE som i den opprinnelige sertifiserte versjonen. SERTIT har som mål å etablere et vedlikeholdsprogram for sertifikater, men dette vil først skje på et senere tidspunkt.

Når vedlikeholdsprogrammet er etablert kan oppdragsgiver, i forbindelse med endringer av TOE, vedlikeholde TOE under sertifiseringsordningen uten de samme kostnadene som ved en formell re-evaluering. Hensikten med vedlikeholdsprogrammet er å opprettholde anerkjennelsen av sertifikatet uten for store kostnader og for stor risiko.

10 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
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
EWP	Evaluation Work Plan, (evalueringsplan)
NSM	Nasjonal sikkerhetsmyndighet
PP	Protection Profile, (kravspesifikasjon)
QP	Qualified Participant, (Kvalifisert sertifiseringsmyndighet)
SERTIT	Sertifiseringsmyndigheten for IT-sikkerhet
ST	Security Target, (sikkerhetsobjekt, løsningsspesifikasjon)
TIN	Task Initiation Notice (orientering om evalueringsoppdrag)
TOE	Target of Evaluation, (evalueringobjekt)

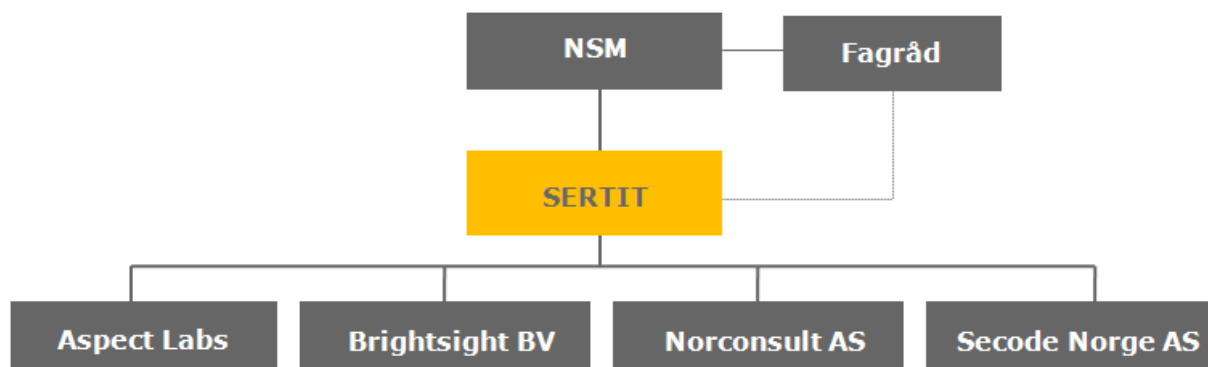
11 Referanser

- [1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, gjeldende versjon.
- [2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, gjeldende versjon.
- [3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, gjeldende versjon.



- [4] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, gjeldende versjon.
- [5] CCRA, "Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security", 23 May 2000.
- [6] Common Evaluation Methodology for Information Technology Security, Part 1: Introduction and general model, gjeldende versjon.
- [7] FOR-2001-07-01-744, Forskrift av 1. juli 2001 nr. 744 om informasjonssikkerhet, Forsvarsdepartementet, jf. kgl.res. av 29. juni 2001 nr. 721.
- [8] FOR-2001-07-01-753, Forskrift av 1. juli 2001 nr. 753 om sikkerhetsgraderte anskaffelser, Forsvarsdepartementet, jf. kgl.res. av 29. juni 2001 nr. 721.
- [9] FOR-1998-12-11-1193, Forskrift om offentlige arkiv, 1999-01-01, Kultur- og kirkedepartementet.
- [10] FOR-1999-12-01-1566, Forskrift om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver, 2000-01-01, Kultur- og kirkedepartementet.
- [11] FOR-1972-03-17-3352, Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (Beskyttelsesinstruksen).
- [12] ISO/IEC Guide 27:1983, "Guidelines for corrective action to be taken by a certification body in the event of misuse of its mark of conformity"
- [13] LOV-1967-02-10 nr 00, Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven), Justis- og politidepartementet.
- [14] LOV-2000-04-14-31, Lov om behandling av personopplysninger (personopplysningsloven), 14. april 2000, Justis- og politidepartementet.
- [15] LOV-1998-03-20-10, Lov om forebyggende sikkerhetstjeneste (Sikkerhetsloven), 18. april 1997, Forsvarsdepartementet.
- [16] NS-EN ISO/IEC 17025, Generelle krav til prøvings- og kalibreringslaboratoriers kompetanse, Norges Standardiseringsforbund (NSF), 1999.
- [17] NS-EN 45011, Generelle krav til organer som har systemer for produktsertifisering (ISO/IEC Guide 65), utgave 2, 1998, Norges Standardiseringsforbund (NSF).
- [18] Sd 003, Krav til evalueringsfirma, v. 3.0, 02.07.2007, SERTIT.
- [19] Sd 027E, Application for certification, v. 1.0, 16.09.2004, SERTIT.
- [20] Sertifisering av IT-sikkerhet i produkter, systemer og organisasjoner (sluttrapport), 13. november 1997, Rådet for IT-sikkerhet.

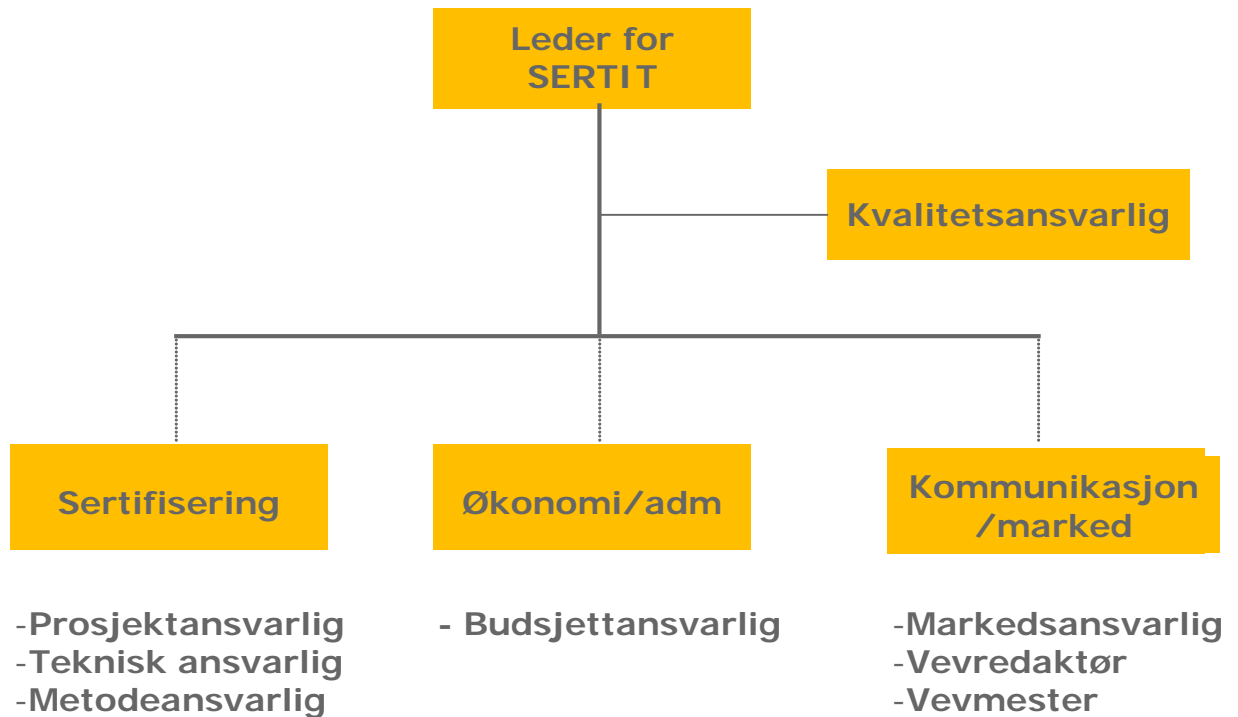
Vedlegg A: Organisering av sertifiseringsordningen



SERTIT utøver tilsynsansvar overfor fire godkjente kommersielle evalueringsinstanser; Aspect Labs, Brightsight BV, Norconsult AS og Secode Norge AS. SERTIT utformer rammevilkår for sertifisering av IT-sikkerhet i Norge, og utsteder sertifiseringsrapporter og sertifikater på bakgrunn av sikkerhetsevaluering utført av evalueringsinstansene.

SERTIT er lagt til Nasjonal sikkerhetsmyndighet (NSM), der SERTITs virksomhet er organisert som en del av direktoratet. NSM koordinerer de forebyggende sikkerhetstiltak og kontrollerer sikkerhetstilstanden i Norge. NSMs ansvarsområde er dels gitt gjennom lov om forebyggende sikkerhetstjeneste og dels gjennom de årlige tildelings- og iverksettelsesbrevene.

Vedlegg B: Organisasjonskart for SERTIT – funksjoner og roller



Leder for SERTIT er ansvarlig for den daglige ledelsen av ordningen, og har attestasjonsmyndighet. SERTIT er bemannet med 3,5 årsverk. SERTITs virksomhet er innrettet i tråd med kravene som er definert i NS-EN 45011 [17], og det er pekt ut en person med ansvar for kvalitetssystemet. Vedkommende er ansvarlig for å sikre at det er etablert, implementert og vedlikeholdt et kvalitetssystem. Tilsyn av EVIT er også omfattet av kvalitetssystemet. Kvalitetsansvarlig rapporterer til leder for SERTIT.

Sertifiseringsaktivitetene håndteres i de enkelte prosjektene ved at det pekes ut en ansvarlig prosjektansvarlig i henhold til fastlagte kriterier og prosedyrer. Vedkommende er blant annet ansvarlig for å føre tilsyn med sikkerhetsevalueringen og utarbeide sertifiseringsrapport og sertifikat. Prosjektansvarlig rapporterer til leder for SERTIT. Det er leder for SERTIT som gir endelig godkjenning av sikkerhetsevalueringen og sertifiseringsresultatet.

De øvrige oppgavene i virksomheten innen økonomi/administrasjon og kommunikasjon/marked foregår dels internt i SERTIT eller i NSM. Rapportering skjer til leder for SERTIT.

Vedlegg C: Mandat for SERTIT

For nærmere informasjon om bemyndigelse for SERTITs drift og ordningens forankring vises til dokumentene fra NHD av 01.02.1999 og 14.04.1999, begge med ref 98/4561-F-ITK eja/lem, i kvalitetssystemets dokumentoversikt.

1. Den offentlige sertifiseringsmyndigheten for IT-sikkerhet, SERTIT er organisert som en del av Nasjonal sikkerhetsmyndighet. Aktivitetene etatsstyres gjennom styringsdialogen med Forsvarsdepartementet (FD) og Justis- og politidepartementet (JD)
2. For å møte behovene i offentlig og privat sektor skal SERTIT utføre følgende oppgaver:

Administrative oppgaver

- a. Være sekretariat for fagrådet for SERTIT,
- b. Utarbeide budsjetter og føre kontroll med økonomien,
- c. Registrere for sertifisering alle evalueringer under ordningen,
- d. Holde oversikt over faglig status for evalueringsfirmaenes ansatte,
- e. Utstede sertifikater for produkter og systemer,

Utadrettede oppgaver

- f. Informere om ordningen,
- g. Godkjenne pressemeldinger og liknende utsagn angående ordningen,
- h. Dokumentere og offentliggjøre en beskrivelse av organisasjonsstruktur, rammevilkår, regler og prosedyrer i ordningen, samt sørge for nødvendig oppdatering,

Faglige oppgaver

- i. Godkjenne evalueringsfirmaer (EVIT),
- j. Føre tilsyn med godkjente evalueringsinstanser, kontrollere deres arbeid og hvordan arbeidet utføres, deres etterlevelse av ordningens bestemmelser og deres evne til å oppnå ordningens målsettinger,
- k. Sørge for at alle prosedyrer og rutiner hos evalueringsfirmaene (EVIT) er i henhold til bestemmelsene i CCRA, og sikre at sensitiv informasjon om produkter, systemer og beskyttelsesprofiler (og løsningsspesifikasjoner) i evalueringen håndteres og beskyttes i henhold til kravene samt at disse rutinene følges,
- l. Utvikle og vedlikeholde en norsk evalueringsmetodikk og sikre konsistens med de til enhver tid eksisterende internasjonale kriterier og metoder,
- m. Gi råd, støtte og standarder for opplæring hos evalueringsinstansene,

- n. Stadfeste hensiktsmessigheten i grunnlaget for evaluering av produkter og systemer, vedta arbeidsprogrammer for evaluering og utgi lister over hva som skal produseres og leveres i forbindelse med en sertifisering,
- o. Lage sertifiseringsrapport for hver fullført og godkjent evaluering,
- p. Bekrefte evalueringsresultatet under ordningen og angi detaljer om sertifiserte og registrerte produkter i en egen liste over sertifiserte produkter,

Internasjonale oppgaver

- q. Etablere forbindelser med nasjonale og internasjonale organer vedrørende gjensidig anerkjennelse av sertifikater,
- r. Representere Norge i CCRA som forpliktet gjennom arrangementet.