



Sertifisering av IT-sikkerhet  **SERTIT**



Hensikten med sertifiseringsordningen for IT-sikkerhet

CCRA:
Arrangement on the Recognition
of Common Criteria Certificates
in the field of Information
Technology Security.

CC:
Common Criteria for Information
Technology Security Evaluation

CEM:
Common Evaluation Methodology
for Information Technology
Security Evaluation

Sertifisering innebærer en uavhengig tredjeparts vurdering av hvilken grad av tillit sikkerheten i et produkt eller system har. Sertifiseringen er basert på formelle kriterier og metodikk som er internasjonalt anerkjent. Ved en sertifisering blir produktet eller systemet gjenstand for en grundig evaluering som gir tillit til at sikkerhetsfunksjonaliteten er implementert korrekt og at det ikke finnes kjente svakheter.

Sertifiseringsordningen for IT-sikkerhet er etablert for å dekke industriens og myndighetenes behov for en kostnadseffektiv og rasjonell sikkerhetsmessig evaluering og sertifisering av IT-produkter og -systemer. Sertifisering av norske produkter vil gi norske produsenter mulighet til å konkurrere der hvor det etterspørres sertifiserte løsninger.

Det benyttes standardiserte krav og metodikk slik at en utvikler skal være sikker på at utfallet av en evaluering vil alltid være det samme. De generelle kravene, både til funksjonalitet og tillit, er definert i CC, mens CEM gir metodikken for hvordan krav skal forstås og evalueres.

Norge har i en internasjonal samarbeidsavtale (CCRA), forpliktet seg til å anerkjenne sertifikater som er utstedt av kvalifiserte sertifiseringsmyndigheter i andre land.



Om SERTIT

SERTIT er den offentlige sertifiseringsmyndigheten for IT-sikkerhet i produkter og systemer.

SERTITs oppgave er å føre tilsyn med evalueringene, utarbeide sertifiseringsrapporter og utstede sertifikater. SERTIT er også ansvarlig for å utforme rammevilkår og regler for ordningen, og se til at reglene etterleves.

SERTIT rapporterer til en uavhengig styringskomité og er lagt til Nasjonal sikkerhetsmyndighet (NSM), som holder til på Kolsås i Bærum.

For mer informasjon om evaluering og sertifisering, CC eller muligheten for å bli EVIT, kontakt SERTIT:

SERTIT

Postboks 14

1306 Bærum postterminal

e-post: post@sertit.no

Internett: sertit.no

Telefon: 67 86 40 00

Telefaks: 67 86 40 09



Om EVIT

Evalueringsfirma (EVIT) 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 evalueringsaktiviteter. Evalueringsvirksomheten er regulert gjennom bestemmelsene i CCRA og nasjonale krav fastlagt av SERTIT.

Evalueringsfirmaene skal evaluere IT-produkter og -systemer på et forretningsmessig grunnlag i henhold til internasjonale standarder. For å bli godkjent som EVIT, må firmaene være akkreditert som testlaboratorium etter ISO 17025.

Følgende firma er godkjent for å utføre evalueringer under sertifiseringsordningen:

■ Norconsult AS
Vestfjordgaten 4
1338 Sandvika

Telefon: 67 57 14 10
e-post: evit@norconsult.no
Internett: evit.norconsult.no

■ Secode Norge AS
Serviceboks 721
4808 Arendal

Telefon: 37 05 81 00
e-post: marked@secode.com
Internett: secode.no



Generelt om evaluering og sertifisering

Evaluering og sertifisering skjer normalt i tre trinn:

- **Forberedelse:** I denne fasen utarbeides og ferdigstilles grunnlaget for evalueringen.
- **Evaluering:** Består normalt av to trinn. I første trinn avklares det om alle forutsetninger for å gjennomføre evaluering og sertifisering er oppfylte. I andre trinn gjennomføres selve evalueringen som resulterer i en teknisk evalueringsrapport.
- **Sertifisering:** SERTIT vurderer den tekniske evalueringsrapporten og om de fremlagte resultater er tilstrekkelige og konsistente. SERTIT avslutter sertifiseringen med å utstede en sertifiseringsrapport og et sertifikat.

Med produkt og system menes:

- Et produkt er en dataløsning med programvare og/eller maskinvare som kan settes inn i et system. Et eksempel på et produkt, kan være en database som selges til ulike kunder som kan ha ulike systemer.
- Et system er en spesifikk IT-installasjon, eller konfigurasjon med et definert bruksområde og brukermiljø. Et eksempel på et system, er et kontorstøttenettverk med tilkoblede arbeidsstasjoner og servertjenester.
Et system evalueres mot forhåndsdefinerte sikkerhetskrav som gjelder for den spesifikke installasjonen, i det gitte brukermiljøet.

Evaluering:

En teknisk undersøkelse av om et produkt eller system oppfyller gitte krav

Sertifisering:

Typegodkjenning av et produkt eller system basert på en gjennomført evaluering. Resultater i at det utstedes et sertifikat.



SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet
SERTIT, P.O. Box 14, N-1306 Bærum postterminal
Telefon: 67 86 40 00 Fax: 67 86 40 09
E-post: post@sertit.no Internett: sertit.no