



viden

Common Criteria vejledning til leverandører



IT- og Telestyrelsen

Ministeriet for Videnskab
Teknologi og Udvikling

Kolofon



IT- og Telestyrelsen

Holsteinsgade 63
2100 Kbh. Ø

Telefon 3545 0000
Telefax 3545 0010

E-mail: itst@itst.dk
www.itst.dk

Indholdsfortegnelse



1	Formål med vejledningen	4
2	Introduktion til Common Criteria	5
2.1	Forkortelser og terminologi	5
3	At anvende Common Criteria	7
3.1	Forretningsmæssige overvejelser	8
3.1.1	Hvilke fordele opnås ved anvendelse af Common Criteria	9
3.1.2	Hvilke ulemper er der ved anvendelse af Common Criteria	9
4	Fremgangsmåde når I har taget beslutningen	10
4.1	Evalueringsproces	11
4.2	Håndtering af produkter med kort livstid, med stor foran- dringshyppighed, eller af flere produkter	12
5	Beskrivelse af Common Criteria	13
5.1	Protection Profile og Security Target	13
5.1.1	Protection Profile	13
5.1.2	Security Target	15
5.2	Opbygning af krav	16
5.2.1	Funktionelle sikkerhedskrav	16
5.2.2	Verifikationskrav og evalueringsniveauer	17
5.2.2.1	Security Assurance Requirements	17
5.2.2.2	Evalueringsniveauer	18
6	Links	19

1 Formål med vejledningen



IT- og Telestyrelsen har udarbejdet denne vejledning til leverandører, som gerne vil introduceres til Common Criteria. Vejledningen henvender sig hovedsageligt til ledelsen, men udviklere og andre kan også have gavn af at læse den. Vejledningen er en introducerende information om Common Criteria, og der lægges vægt på forretningsprocessen samt fordele og ulemper.

Du kan læse mere om Common Criteria på:
<http://www.commoncriteriaportal.org>

Vejledningen beskriver kort, hvordan Common Criteria kan anvendes til at designe sikkerheden i it-produkter. Derudover giver vejledningen information om certificering af it-produkter baseret på Common Criteria.

Common Criteria (CC) er en internationalt anerkendt ISO-standard (ISO 15408)¹, som kan benyttes til design og sikkerhedscertificering af it-produkter. CC bruges til at formulere en standardiseret beskrivelse af sikkerheden i et it-produkt/system.

Som leverandør af it-systemer kan I anvende Common Criteria til at designe sikkerhedsfunktionalitet. CC angiver en systematisk metode til design af sikkerhedsfunktioner, og "tvinger" jer igennem en række overvejelser, som er nødvendige for at sikre kvaliteten i implementeringen og den løbende udbedring af fejl.

Det er vigtigt at påpege, at en Common Criteria certificering ikke beviser at et produkt er sikkert/giver sikkerhed, og at evalueringsniveauet ikke er et mål for, hvor sikkert et produkt er. Evalueringen giver en grad af vished for at sikkerhedsfunktionaliteten svarer til det miljø, produktet skal anvendes i, er veldokumenteret og implementeret korrekt.

Det internationale samarbejde om Common Criteria-certificeringer sker via Common Criteria Recognition Arrangement (CCRA). Medlemmer i CCRA er enten certifikatforbrugende eller certifikatudstedende. Certifikatudstedende lande fører tilsyn med sit eget lands evalueringslaboratorier, mens certifikatforbrugende lande ikke selv har et certificeringssystem. 24² lande har formelt anerkendt standarden ved at deltage i CCRA. Videreudviklingen af CC sker også i regi af CCRA.

Danmark er medlem af CCRA som certifikatforbrugende medlem. Hvis jeres produkt skal certificeres indebærer dette dermed, at evalueringen skal foretages af et evalueringslaboratorium fra et andet land.

2.1 Forkortelser og terminologi

Der findes langt flere betegnelser end der er plads til i denne vejledning. Du kan finde en ordliste i User Guide, som kan hentes her: <http://www.commoncriteriaportal.org/public/files/ccusersguide.pdf>. Nedenfor beskrives kort de grundlæggende termer.

It-sikkerhedsprodukt: et it-sikkerhedsprodukt i CC-terminologi defineres som et produkt som giver sikkerhed for enten dets miljø eller sig selv. I praksis betyder det, at stort set alle it-produkter kan betragtes som et it-sikkerhedsprodukt og dermed kan blive CC-certificeret. I denne vejledning skriver vi derfor kun "it-produkt" eller "it-system".

Evaluering / certificering: Common Criteria specificerer kravene for at evaluere et it-system. Certificering er resultatet af en succesfuld evaluering. Evaluering er processen, hvor produktet sammenlignes med CC-standard. Evalueringen udføres af et evalueringslaboratorium (Common Criteria Testing Laboratory - CCTL), som typisk er et privat firma.

Certificeringsmyndighed (Certification Body): er typisk en statslig myndighed, som fører tilsyn med CC i det pågældende land. Certifice-

1 Common Criteria standarden er et dokument på ca. 600 sider, som kan hentes gratis på <http://www.commoncriteriaportal.org/>

2 På udgivelsestidspunktet for denne vejledning var Australien, Canada, Frankrig, England, Holland, Japan, Norge, Spanien, Sydkorea, New Zealand, Tyskland og USA certifikatudstedende medlemmer, mens Danmark, Finland, Grækenland, Indien, Israel, Italien, Singapore, Sverige, Tjekkiet, Tyrkiet, Ungarn og Østrig var certifikatforbrugende medlemmer. En opdateret liste over medlemslande kan altid findes på <http://www.commoncriteriaportal.org/>



ringsmyndigheden gennemgår evalueringslaboratoriernes arbejde, og hvis alt er i orden, certificerer it-produkter. Certificeringsmyndigheder findes kun i certifikatudstedende lande og altså ikke i Danmark.

Protection Profile (PP): er et centralt dokument i Common Criteria evalueringsprocessen. En PP skrives typisk af brugere og definerer en slags standard for en bestemt type produkt. For eksempel har NSA udarbejdet en række PP'er for forskellige slags firewalls. Der findes også PP'er for operativsystemer, databaser, smartcards, printere mm.

Security Target (ST): er også et centralt dokument i evalueringsprocessen og produceres af leverandøren. I nogle tilfælde udarbejdes ST dog i samarbejde med kunden. ST definerer TOE'en, trusler imod TOE, dets sikkerhedsmål, miljøet som ST bruges i, de SFR'er og SAR'er som det overholder samt EAL.

Target of Evaluation (TOE): er den del af it-produktets funktioner som skal evalueres. Det er ikke nødvendigt at evaluere hele produktet med alle dets funktioner. En sammenhængende delmængde er nok, så længe at produktet kan konfigureres til kun at bruge den pågældende delmængde. Dog skal TOE'et i dag dække den funktionalitet, som en bruger normalt vil forvente. I evalueringsprocessen vurderes TOE'ens omgivelser og truslerne herfra. En TOE kan bestå af hardware, firmware og/eller software og kan inkludere flere it-produkter.

Evaluation Assurance Level (EAL): Angiver hvor grundigt sårbarhedsanalysen af TOE'et skal være. Der er syv niveauer: EAL1 til EAL7. Hvert niveau er defineret ved en "pakke" af SAR (Security Assurance Requirements).

Security Functional Requirements (SFR): definerer individuelle sikkerhedsfunktionalitetskrav i et it-produkt. For eksempel at administratorer kan blive nægtet adgang til produktet efter et antal bestemte forsøg på autentifikation. CC præsenterer et standardkatalog af sådanne funktioner. Listen af SFR'er kan variere fra et TOE til et andet, også selvom de to produkter er af samme type (f.eks. to firewalls). Selvom CC ikke foreskriver, hvilke SFR'er der skal inkluderes i et Security Target, viser CC dog hvilke afhængigheder der er, f.eks. at en korrekt fungerende funktion (eks. adgangskontrol ift. roller) er afhængig af en anden funktion (eks. evnen til at identificere individuelle roller).

Security Assurance Requirements (SAR): definerer verifikationsniveau og krav. CC præsenterer et standardkatalog af sådanne krav. Et EAL-niveau består af en specifik samling (pakke) af SAR'er. SAR'er dækker hele udviklingsprocessen og selve produktevalueringen.

I må påregne, at evalueringsprocessen tager mange måneder, og at der skal bruges væsentlige udgifter til at få certificeret et produkt. ECMA³ anslår, at prisen for en evaluering er mellem 10% og 40% af udviklingsprisen. Alex Ragen⁴ anslår, at en normal, amerikansk certificering koster omkring 500.000 US dollar. Men prisen afhænger selvfølgelig både af it-systemets omfang og type, EAL (1 er billigst, 7 er dyrest), hvilket evalueringslaboratorium der benyttes samt andre faktorer.

Certificering sker på basis af en given konfiguration af systemet. Det betyder, at certificeringen alene dækker den aktuelle version af systemet. Efter at evalueringsprocessen er overstået, skal I derfor allerede begynde at tænke på, om den/de næste versioner af produktet skal certificeres. Mange evalueringslaboratorier tilbyder vedligeholdelsesordninger. Særskilt certificering af udviklingsmiljøet samt opdeling i komponenter (component TOE's) muliggør ligeledes ofte en betydelig reduktion i omkostningerne til vedligeholdelse af certificeringen.

Bemærk at Common Criteria kan udgøre et nyttigt værktøj i forbindelse med udvikling og design af it-systemer uanset om I vælger at certificere jeres produkt. CC kan nemlig bruges til at designe mere sikre produkter og vil ofte føre til et løft af den generelle modenhed vedrørende styring af udviklingsprocessen. CC definerer nogle metoder til, hvordan man gør dette, og disse metoder kan bruges på it-produkter.

Hvilke kunder lægger vægt på Common Criteria?

En typisk indkøber, som lægger vægt på CC eller efterspørger CC kan have et eller flere af følgende kendetegn:

- Er forsvaret, den finansielle sektor eller andre kritiske myndigheder med høje sikkerhedskrav.
- Er en offentlig myndighed, som er pålagt at kræve CC. Nogle landes offentlige administration (eksempelvis i USA) må kun indkøbe CC-certificerede produkter, hvis de findes.
- Er for eksempel en indisk eller asiatisk indkøber, hvor CC-udbredelsen går meget stærkt.
- Er en virksomhed, der benytter offshore outsourcing.
- Er et datacenter eller andre slags virksomheder med høje sikkerhedskrav.
- Er en organisation, som prioriterer sikkerhed i produkter som firewalls, arbejdsstationer (herunder hjemme- arbejdspladser), servere mv.
- Er en organisation, som er kendt for strategiske overvejelser og høj grad af modenhed, som f.eks. har it-strategiske overvejelser om design og implementering af it-arkitektur, systemplatforme og it-applikationer.

³ European Computer Manufacturers Association – en international organisation med medlemmer fra både Europa, USA og Japan.

⁴ Alex Ragen har skrevet Manager's Guide to the Common Criteria, www.alexragen.com



3.1 Forretningsmæssige overvejelser

Common Criteria adresserer både proces og resultat, hvilket betyder at både selve udviklingsprocessen og det færdige produkt evalueres. På denne måde sikres det, at sikkerheden er tænkt ind i udviklingsprocessen. Der lægges vægt på en stram styring af udvikling og test samt produktion og vedligeholdelse.

Common Criteria giver flere fordele, men det kræver dog en vis modenhed for at få fuld udnyttelse af fordelene. En typisk leverandør, som vil have gavn af at certificere et eller flere af sine produkter vil have et eller flere kendetegn:

- rimelig grad af modenhed
- en international kundekreds
- et kundesegment, der efterspørger sikkerhed og er villige til at betale for sikkerhed
- leverandør af kritiske systemer til f.eks. forsvaret, sundhedsområdet eller proceskontrollsystemer
- leverandører af egentlige it-sikkerhedsprodukter eksempelvis log management, firewalls, antivirus, Intrusion Detection systemer
- leverandør af essentielle ydelser til f.eks. hele det offentlige område eks. infrastruktur eller webservices.

Før din virksomhed går ind i en krævende evalueringsproces skal I overveje, om det er realistisk at jeres produkt skal CC-certificeres. Det kræver en rimelig høj grad af modenhed, I skal have 100% styr på udviklingsprocesserne, og processerne skal være veldokumenterede. Sikkerhed skal være tænkt ind jeres design fra starten af.

Det er også vigtigt at vurdere jeres kunders behov for CC-certificerede produkter. Vurder hvor vigtigt sikkerhed er for netop jeres kunder. Er jeres kunder villige til at betale for sikkerhed og stiller de eksplicitte krav om sikkerhed, så peger det i retning af, at I skal vælge at få CC-certificeret jeres produkt.

Derudover er det vigtigt, at der afsættes de finansielle ressourcer og

Eksempler på produkter som er Common Criteria certificerede

De produkter, som typisk certificeres, er blandt andet:

- 1 multifunktionsenheder (f.eks. printere, scan-nere, kopimaskiner)
- 2 smartcards og smartcardsrelaterede systemer
- 3 firewalls
- 4 VPN
- 5 databaser
- 6 PKI-systemer / Key Management systemer
- 7 operativsystemer (både kommercielle og open source)
- 8 telefonadministrations-systemer
- 9 adgangskontrol-systemer og enheder
- 10 krypteringssystemer
- 11 systemer/produkter med digital signatur teknologi
- 12 IDS
- 13 netværk og netværksrelaterede systemer/produkter
- 14 bevægelsessensorer
- 15 biometriske systemer
- 16 sikre mailing-systemer/ mailinglists
- 17 VoIP-løsninger
- 18 kommunikations-systemer
- 19 databaseskyttelse

På <http://www.commoncriteria.org/public/developer/index.php?menu=6> kan I finde en liste over Common Criteria evaluerede produkter.



medarbejderressourcer, som er nødvendige for at opnå en succesfuld evaluering. Det kan anbefales, at I fra starten udpeger (eller ansætter) en projektleder, som varetager hele evalueringsprocessen.

3.1.1 Hvilke fordele opnås ved anvendelse af Common Criteria

Tillid til it-produkter

En Common Criteria-certificering fremmer tillid til it-produkter, da de er evalueret af en uafhængig part ifølge en internationalt gensidigt anerkendt standard. For en leverandør giver dette en ekstra kvalitetssikring og unikke muligheder for at bruge certificeringen som et kvalitetsstempel i salgsøjemed.

Produkter kan bruges i følsomme områder

En Common Criteria-certificering giver en garanti for at produktet er sikkerhedstestet. Med tiden vil flere kræve, at it-produkter er blevet sikkerhedstestet.

International anerkendelse

Et Common Criteria-certifikat⁵ er gensidigt anerkendt i alle lande, som er medlem af CCRA. Dette er en vigtig fordel i forhold til marketing på det internationale område.

Værktøj til design af sikkerhed

De leverandører, som anvender CC-kriterierne, vil have mulighed for at forbedre deres proces for design af sikkerheden i systemer og produkter. Med Common Criteria får leverandøren et værktøj, der kan bruges til at udvikle it-produkter under hensyn til det sikkerhedsmæssige aspekt.

3.1.2 Hvilke ulemper er der ved anvendelse af Common Criteria

Ressourcekrævende

Det er ressourcekrævende både i medarbejderressourcer og udgifter at blive certificeret efter Common Criteria. Produkter, som ofte opgraderes, er endnu mere ressourcekrævende at få CC-certificeret.

Længere tid til markedet

Ved omfattende evalueringsprocedurer er der en risiko for en betragtelig sagsbehandlingstid før et produkt er godkendt. Dette kan betyde en væsentlig forlængelse af nye produkters vej til markedet, og dermed en bevarelse af eksisterende, forældede løsninger. Ved at tænke certificering ind fra starten af udviklingsforløbet kan tiden, det tager at certificere produktet dog reduceres væsentligt.

Skal benytte andet lands evalueringslaboratorium

Da Danmark kun er certifikatforbrugende medlem af CCRA, vil danske leverandører, der ønsker at få certificeret deres produkt, være henvist til at benytte et certifikatudstedende lands laboratorium for at få evalueret deres produkt.

⁵ Til og med EAL4.

Når I først har taget beslutningen, om at jeres produkt skal Common Criteria certificeres, skal I fortsætte med nedenstående punkter.

1. Definer det produkt I vil have certificeret

Har I flere forskellige versioner af jeres produkt, skal I vælge hvilken version eller kommende version, der skal certificeres. Det kan også være, at det kun er en del af jeres produkt, I vil have certificeret. Eller det kan være, at jeres produkt kun er i designfasen. I alle tilfælde kan det være en hjælp for jer allerede nu at få hjælp af et konsulentfirma, som har specialiseret sig i Common Criteria vejledning.

2. Specificer hvilken funktionalitet jeres produkt skal have

Det kan være, at jeres kunder har stillet nye, højere krav eller at I forudser dette. Det kan også være, at I bliver nødt til at kigge på, hvilken funktionalitet jeres konkurrenters produkter har. Undersøg også, om der allerede er udarbejdet en Protection Profile for et lignende produkt eller om et tilsvarende produkt er certificeret.

En liste over Protection Profiles kan findes her:

<http://www.commoncriteriaportal.org/public/developer/index.php?menu=7>

En liste over evaluerede produkter kan findes her:

<http://www.commoncriteriaportal.org/public/developer/index.php?menu=6>

3. Bestem hvilket EAL jeres produkt skal evalueres til

Overvej hvilket niveau jeres produkt skal evalueres til. Det kan være det giver sig selv ud fra de krav I eller jeres kunder har til produktet, men ellers kan det være en god ide, at se hvilket EAL-niveau lignende produkter eller konkurrenters produkter har, eller om der findes Protection Profiles, som lige passer til jeres produkt. Overvej også hvor lang tid og hvor ressourcekrævende evalueringsprocessen må være. Jo højere EAL-niveau, desto længere tid og flere ressourcer vil I komme til at bruge. Generelt vil antallet af identificerede sårbarheder i evalueringsprocessen være proportionalt med EAL-niveauet. Tiden det tager, at gennemføre en succesfuld evaluering er i høj grad afhængig af, hvor mange gange evalueringen skal gentages på grund af fejl.

4. Bestem hvilket evalueringslaboratorium I vil bruge

I skal overveje, hvilket evalueringslaboratorium, I vil benytte, og om I både vil benytte det til konsulenthjælp før evalueringen og til at udføre evalueringen eller kun en af delene.

I skal blandt andet overveje følgende:

- Skal laboratoriet være tæt på for at minimere rejseomkostninger og tidsforbrug?
- Skal laboratoriets medarbejdere tale skandinavisk eller engelsk?
- Skal laboratoriet have evalueret lignende produkter/teknologi eventuelt med samme EAL? Det anbefales, at vælge et laboratorium med erfaring med lignende produkter.
- Skal laboratoriet have erfaring med lignende produkter/teknologi (dog uden at have evalueret sådanne)?
- Skal laboratoriet også kunne tilbyde konsulenttydelser såsom hjælp til at skrive Security Target? Man bør overveje, at holde de to ydelser adskilt.



- Skal certificeringsprocessen gå hurtigt? Nogle laboratorier er hurtigere end andre.
- Hvad må det koste? Dette afhænger typisk af, hvor hurtigt det skal gå, og hvor højt EAL skal være.
- Vil evalueringslaboratoriet give jer alle beviser/materialer/data, som er genereret under evalueringsprocessen? Det anbefales, at dette indgår som et punkt i kontrakten.
- I hvilket land er jeres største marked? Det er en fordel, at få certificeret produktet i det land, som er jeres største marked.
- Skal laboratoriet tilbyde vedligeholdelsesordninger, således at det er lettere at få certificeret nye versioner af jeres produkt?

I kan finde en liste over evalueringslaboratorier her:

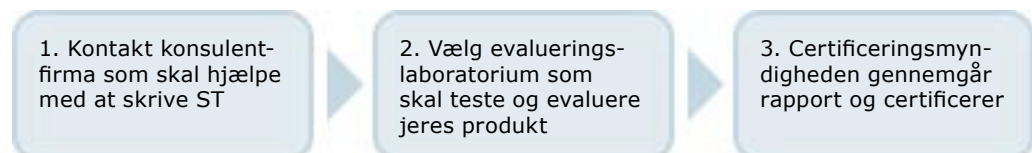
<http://www.commoncriteriaportal.org/public/developer/index.php?menu=9>

5. Udarbejd dokumentation

Det er vigtigt, at I har styr på hele jeres udviklingsproces og udarbejder dokumentation for f.eks. designet. Evalueringslaboratoriet skal nemlig bruge en omfattende dokumentation for jeres produkts funktionalitet og udviklingsprocessen. Derudover skal I selvfølgelig udarbejde et Security Target.

4.1 Evalueringsproces

Sådan foregår en typisk evalueringsproces:



1. I kontakter eventuelt et konsulentfirma, som hjælper med at skrive Security Target (ST), beskrive produktet og teste produktet.
2. I vælger et evalueringslaboratorium⁶, der evaluerer produktet og bestemmer om både produkt og dokumentation overholder Common Criteria, produktet testes ifølge verifikationskravene i forhold til EAL-niveau, og der aflægges besøg hos jer og/eller I giver laboratoriet mulighed for at penetrationsteste jeres system. Derefter udarbejder evalueringslaboratoriet en rapport⁷, som indeholder oplysninger om mangler, fejl med videre. Rapporten sendes til certificeringsmyndigheden. I nogle lande er konsulentfirmaet og evalueringslaboratoriet det samme firma (men forskellige afdelinger).

⁶ På www.commoncriteriaportal.org findes en liste over officielle evalueringslaboratorier.

⁷ Evaluation Technical Report (ETR)



3. Certificeringsmyndigheden gennemgår rapporten (ETR) fra evalueringslaboratoriet, og hvis denne godkendes bliver der udstedt et certifikat og udarbejdet endnu en rapport (Evaluation Report – ER). Både certifikat og ER er offentligt tilgængelige dokumenter. ETR indeholder fortrolige oplysninger og bliver derfor normalt ikke publiceret.

I praksis er evalueringsprocessen iterativ. For eksempel kan evalueringslaboratoriet stille spørgsmål til produktet eller dokumentationen, og som svar kan I ændre produktet eller konsulenten kan ændre dokumentationen og derefter genindsende materialet. Hvis evalueringslaboratoriet stadig ikke er tilfreds, skal der foretages nye ændringer osv.

4.2 Håndtering af produkter med kort livstid, med stor forandringshyppighed, eller af flere produkter

Der findes ingen klare procedurer for at "vedligeholde" en certificering – altså for at en ny version af produktet kan certificeres hurtigt. Nogle evalueringslaboratorier tilbyder dog en hurtigere og billigere evalueringsproces for nye versioner af samme produkt, hvor elementer fra den første evaluering kan genbruges, i det omfang ændringerne ikke påvirker disse. For eksempel kan brugerdokumentation ofte genbruges.

Den gældende version af standarden giver desuden mulighed for evaluering af såkaldte component TOE's, som kan være en selvstændig del af et produkt. Hvis nogle dele af produktet er mere statiske, kan det være en fordel at gøre disse til component TOE's, da reevalueringen så kan reduceres til de dele af produktet, der er ændret. Jeres eget ressourceforbrug vil sandsynligvis også kunne minimeres på denne måde.

Den del af evalueringen, der vedrører virksomheden/leverandøren, kan normalt også genbruges. CC giver mulighed for, at de enkelte faser, fra et produkt beskrives til det ender hos kunden, kan certificeres særskilt. Hvis I har flere produkter, der udvikles, testes, produceres og/eller shippes fra samme fysiske lokaliteter og efter samme proces, bør I undersøge, om I eksempelvis vil have fordel af at certificere testafdelingen særskilt, hvis den er fælles for en række produkter, I ønsker certificeret.

Inden du læser dette kapitel, kan det være en god ide, at genopfriske forkortelser og terminologi i afsnit 2.1.

Common Criteria standarden består af tre dele, som alle kan hentes her: <http://www.commoncriteriaportal.org/public/developer/index.php?menu=2>.

- Del 1: Giver overblik og kan bruges som baggrundsinformation og reference for udviklingen af krav og formuleringen af sikkerhedsspecifikationer for TOE'en.
- Del 2: Beskriver Security Functional Requirements (SFR) og kan bruges som reference når redegørelser for funktionelle krav skal fortolkes og til brug for formulering af funktionelle specifikationer i TOE'en.
- Del 3: Beskriver Security Assurance Requirements (SAR) og kan bruges som reference når redegørelser for verifikationskrav skal fortolkes og når niveau og fremgangsmåder for verifikation i TOE'en skal bestemmes.

5.1 Protection Profile og Security Target

I CC opereres der med to centrale dokumenter, som kaldes henholdsvis "Protection Profile" (PP) og "Security Target" (ST):

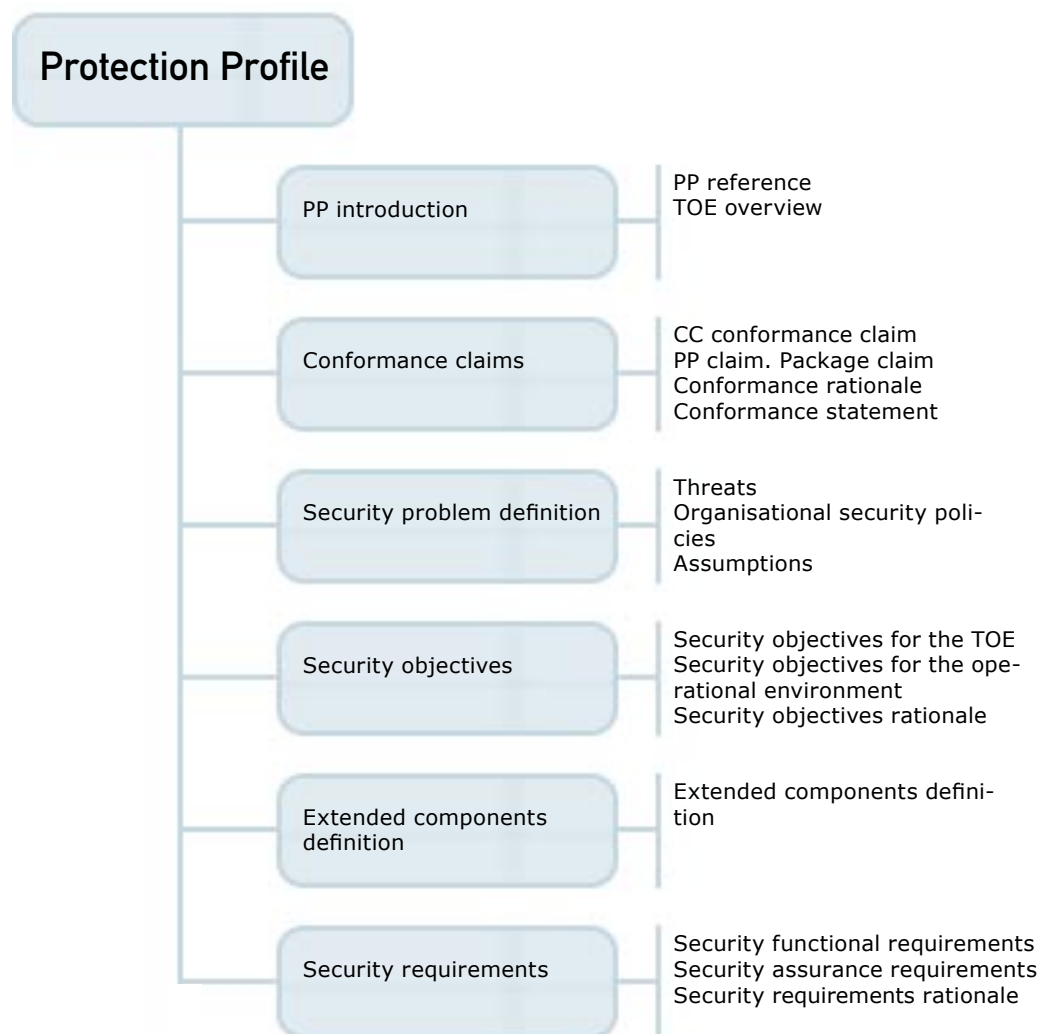
- **Protection Profile:** En PP beskriver de sikkerhedsmæssige krav, der stilles til en bestemt type af systemer.
- **Security Target:** Et ST identificerer et specifikt systems egenskaber i forhold til sikkerhed.

Mens Protection Profiles typisk udarbejdes af brugere, indkøbere eller organisationer (f.eks. offentlige myndigheder) og beskriver sikkerheden i en bestemt type af system, udarbejdes Security Targets af leverandører og adresserer sikkerheden i det produkt, de ønsker certificeret.

5.1.1 Protection Profile

En Protection Profile er en slags standard for sikkerheden i en bestemt type af produkter eller systemer. For eksempel findes der Protection Profiles for firewalls og for hjemmearbejdspladser.

En Protection Profile består af:



Der er allerede udarbejdet en lang række PP'er, som kan findes på <http://www.commoncriteriaportal.org/public/developer/index.php?menu=7>

Som leverandør behøver I ikke udarbejde en Protection Profile, men I kan vælge at udvikle jeres produkt sådan, at det er i overensstemmelse med en eller flere Protection Profiles. Vælger I dette, kan de pågældende PP'er fungere som en slags skabelon for jeres Security Target, og således skal alle krav beskrevet i disse PP'er også optræde i jeres ST. Indkøbere, som søger efter bestemte typer produkter, kan vælge at fokusere udelukkende på produkter, som er evalueret imod specifikke PP'er. Det er netop en af styrkerne ved Common Criteria, da kunden hermed får mulighed for at vurdere produkterne i forhold til et sæt af standardkrav for den pågældende type produkt.

Nogle leverandører vælger dog, først at beskrive deres produkt i en generel Protection Profile eventuelt med hjælp fra deres kernekunder. Derefter skriver de deres Security Target. På den måde er leverandøren med til selv at definere en standard for sikkerhedsfunktionaliteten i en given produkttype.

5.1.2 Security Target

Et Security Target beskriver systemet og grundlaget for evalueringen og følger samme struktur som en Protection Profile. Et ST kan påstå at være i overensstemmelse med nul eller flere PP'er og kan derudover også påstå at opfylde ekstra SFR'er udover dem som er medtaget i de pågældende PP'er. Det er ikke muligt at påstå delvis overensstemmelse med en PP.

Selve Security Target'et underkastes en evaluering, som sikrer, at der er overensstemmelse med målsætningen og funktionaliteten. Et ST fungerer både som en specifikation af sikkerhedsfunktioner, som TOE'en opfylder, og som en beskrivelse af produktet relateret til driftsmiljøet. Indholdet og præsentationen af ST skal specificeres i CC-betegnelser.

Et Security Target består af:





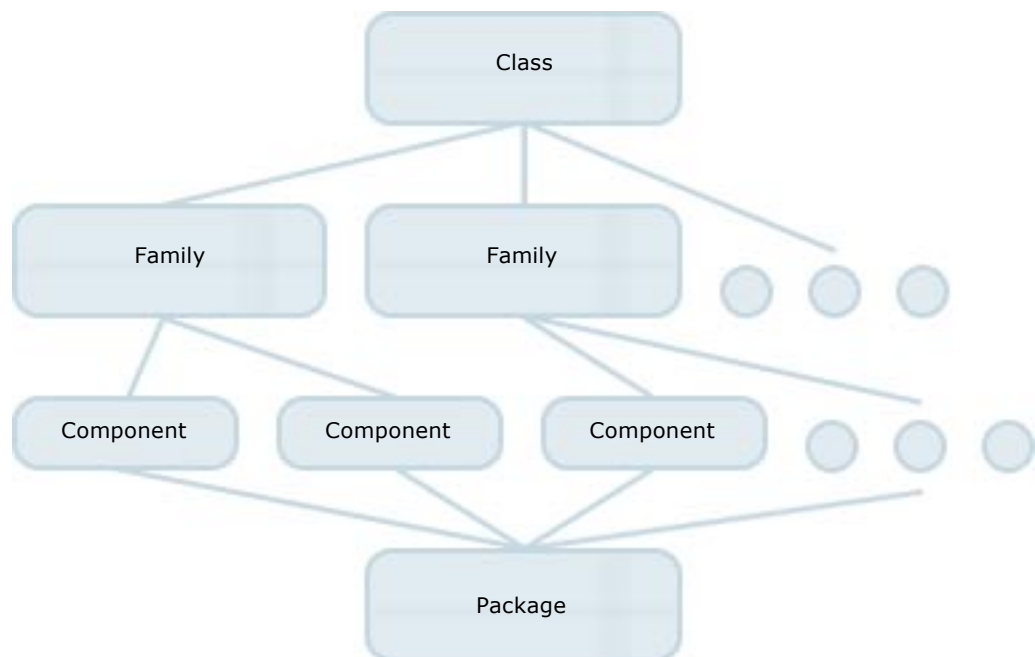
Derudover kan et Security Target også indeholde andre relevante emner eksempelvis styrken af TOE'ens kryptering eller autentifikationsfunktioner.

Et ST offentliggøres, således at jeres kunder kan se hvilke sikkerhedsfunktioner, der er certificeret.

En liste over certificerede produkters Security Targets kan findes her: <http://www.commoncriteriaportal.org/public/developer/index.php?menu=6> Under hvert produkt kan man hente både Security Target og Evaluation Report / Certification Report.

5.2 Opbygning af krav

Common Criteria er bygget op omkring en række potentielle sikkerhedskrav opdelt efter funktionelle behov. Common Criterias sikkerhedskrav (både SFR'er og SAR'er) er hierarkisk delt op i klasser – familier – komponenter – elementer. Alle sikkerhedskrav og afhængigheder mellem kravene er grundigt beskrevet i standarden.



Klasser er grupper af familier, som har samme sikkerhedsmålsætning.

Familier er grupper af komponenter, som har samme sikkerhedsmålsætning.

En komponent beskriver et specifikt sæt af sikkerhedskrav.

Pakker består af komponenter fra en eller flere familier.

5.2.1 Funktionelle sikkerhedskrav

De funktionelle sikkerhedskrav (SFR - Security Functional Requirements) betyder kort "hvad gør produktet". SFR'erne beskriver produktets egenskaber/sikkerhedsfunktioner, og det er SFR'erne man kan bruge til at sammenligne med andre lignende produkter. Når I skal definere, hvilke sikkerhedskrav jeres produkt skal overholde, skal I overveje hvilke trusler, der er imod it-miljøet.



CC-standardens del2 indeholder et katalog af funktionelle sikkerhedskrav, som I selv kan sammensætte til jeres definition af sikkerhedskrav i jeres ST. Man kan også vælge at bruge SFR'er, som ikke er en del af standarden, men dette sker meget sjældent.

Der er defineret 11 SFR-klasser i standarden:

- 1 FAU – Security Audit
- 2 FCO - Communication
- 3 FCS - Cryptographic Support
- 4 FDP - User Data Protection
- 5 FIA - Identification and Authentication
- 6 FMT - Security Management
- 7 FPR – Privacy
- 8 FPT - Protection of the TSF (TOE Security Functions)
- 9 FRU - Resource Utilisation
- 10 FTA - TOE access
- 11 FTP - Trusted Paths/Channels

5.2.2 Verifikationskrav og evalueringsniveauer

I det følgende beskrives verifikationskrav (SAR) og derefter evalueringsniveauer (EAL).

5.2.2.1 Security Assurance Requirements

CC-standardens del3 indeholder et katalog af verifikationskrav. SAR's omhandler evaluering af miljøet, hvori et produkt er udviklet, udsendt og leveret:

- de værktøjer, som bruges til udvikling og vedligeholdelse
- de procedurer, som bruges til at teste og implementere nye funktioner
- kvalitetssikring
- tilbagevendende tests
- klargøring, pakning og levering
- change management cyklus og udbedring af fejl.

SAR's er en evalueringsbeskrivelse af de tiltag, der er taget under udviklingen, evalueringen og leveringen af produktet for at sikre, at der er overensstemmelse med de påståede sikkerhedsfunktioner. Eksempelvis kan en evaluering kræve at al kildekode opbevares i et change management system.

Der er defineret ni SAR-klasser i standarden:

- a) To klasser der indeholder verifikationskrav for PP og ST evalueringer:
- 1 APE - Protection File Evaluation
 - 2 ASE - Security Target Evaluation
- b) En klasse som omhandler vedligeholdelse af verifikation:
- 3 AMA - Maintenance of Assurance Support
- c) Seks klasser hvorfra evalueringsverifikationskrav kan vælges:
- 4 ADV – Development
 - 5 AGD - Guidance Documents
 - 6 ALC - Life Cycle Support
 - 7 ATE - Tests
 - 8 AVA - Vulnerability Assessment
 - 9 ACO - Composition

De ni SAR-klasser er grupperet i tre grupper, som illustreret i boksen.

Ad a) Målet med ASE-klassen er at demonstrere, at ST'et er komplet, konsistent og teknisk velfunderet, og er et godt grundlag for TOE evalueringen. Kravene i klassens familier omhandler TOE beskrivelse, driftsmiljøet, påstande om PP overensstemmelser, TOE sikkerhedskrav og TOE summary specification.



Ad b) AMA-klassen omhandler krav, som først tilføjes efter TOE'en er certificeret. Disse krav kan bruges til at sikre, at TOE'en fortsat overholder ST selvom der foretages ændringer i TOE'en eller i driftsmiljøet.

5.2.2.2 Evalueringsniveauer

Evalueringsprocessen forsøger at stadfæste den grad af tillid, som brugeren kan have til et produkts sikkerhedsfunktioner, gennem kvalitetsstyringsprocesser. Der er syv EAL-niveauer fra EAL1 til EAL7, hvor EAL7 er det højeste og dermed dyreste. De syv evalueringsniveauer er prædefinerede pakker bestående af SAR-komponenter, det vil sige at det er generiske krav, som gælder alle produkter evalueret til et bestemt EAL. Hvis et produkt opfylder flere SAR'er end et EAL-niveau kræver, men ikke nok til at opnå næste niveau, sættes et plus efter niveauet eksempelvis EAL4+.

Et højt EAL-niveau betyder ikke direkte bedre sikkerhed, men kun at den påståede forsikring for sikkerhed i/af TOE'en er blevet valideret mere grundigt. Der er gennemført grundigere sårbarhedsanalyser på de høje niveauer og normalt er antallet af sårbarheder og fejl evalueringlaboratorierne finder, proportionalt med evalueringsniveauet.

EAL1	Funktionalitet bliver testet: Produktet og dets dokumentation gennemgås for at se om de er i overensstemmelse med hinanden. Det stadfæstes at produktet gør, hvad dokumentationen lover.
EAL2	Struktureret testning: Testen inkluderer blandt andet designhistorik og hvordan det er testet.
EAL3	Metodisk test og kontrol: Produktet evalueres i designfasen med uafhængig verificering af udviklernes testresultater. Udviklernes kontrol for sårbarheder, udviklingsmiljøkontroller og produktets muligheder for administration af konfiguration bliver evalueret.
EAL4	Metodisk designet, testet og inspiceret: Dybere analyse af udviklingen og implementeringen. <i>EAL4 kræver, at du som leverandør er villig til at rette problemer allerede i udviklingsprocessen og dette medfører typisk flere omkostninger.</i>
EAL5	Semiformelt designet og testet.
EAL6	Semiformelt verificeret design og testning.
EAL7	Formelt verificeret design og testning.

EAL4 er i praksis det højeste evalueringsniveau et produkt kan opnå, hvis det ikke er bygget specielt til at opnå et højere niveau.

EAL 5-7 kræver endnu mere formalitet i designprocessen og under implementeringen. Der kræves for eksempel analyse af produktets evne til at modstå og håndtere angreb og undgå mulighed for at der kan forekomme kommunikation, der bryder med systemets sikkerhedspolitik. EAL 5-7 er derfor egnet til de produkter, som er bygget med specielle sikkerhedsteknikker, og som følge deraf har disse niveauer sjældent været rettet mod produkter, som distribueres kommercielt. Der er dog en tendens til at indkøbere stiller større krav til evaluering og flere kommercielle produkter er allerede evalueret på EAL5+.

5 Links



<http://www.commoncriteriaportal.org/>

Dette er den officielle hjemmeside for Common Criteria. Her kan du finde selve standarden, introduktionsmateriale, brugervejledning, lister over certificerede produkter, Protection Profiles osv.

[http://standards.iso.org/ittf/PubliclyAvailableStandards/c039690_ISO_IEC_TR_15446_2004\(E\).zip](http://standards.iso.org/ittf/PubliclyAvailableStandards/c039690_ISO_IEC_TR_15446_2004(E).zip)

ISO har udarbejdet denne vejledning i, hvordan man udarbejder Protection Profiles og Security Targets.

<http://www.alexragen.com/>

Alex Ragen har skrevet »Managers Guide to the Common Criteria«, som kan hentes gratis på hans hjemmeside.

<http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-271.pdf>

ECMA har etableret standarden E-COFC Version 2 (Extended Commercially Oriented Functionality Class for Security Evaluation).

<https://www.icsalabs.com/icsa/topic.php?tid=fdghgf54645-ojojoj567>

ICSA Labs certificering