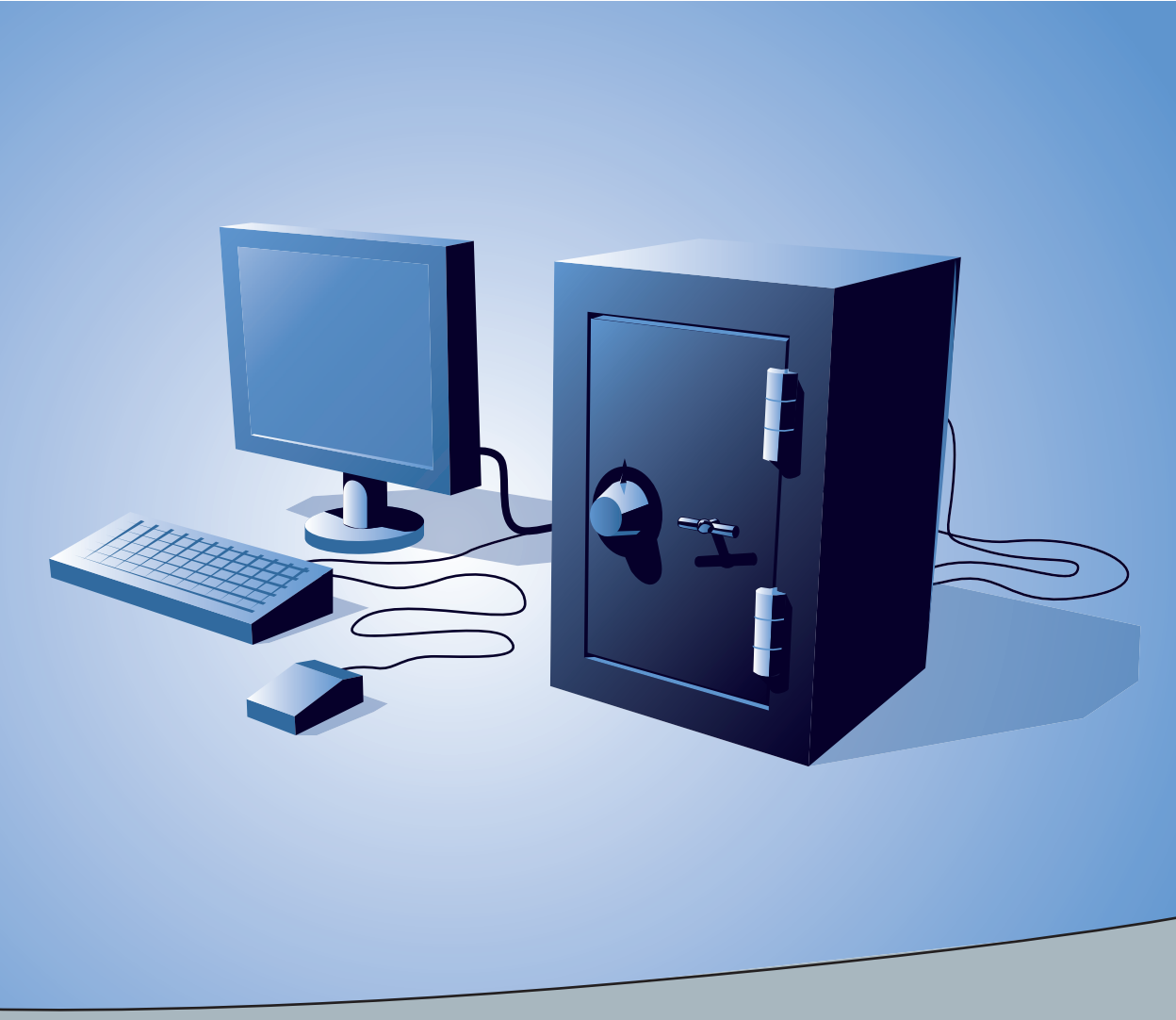


IT-säkerhetsstandarden Common Criteria (CC)

EN INTRODUKTION

KBM REKOMMENDERAR ■ 2007:2

KRISBEREDSKAPS MYNDIGHETEN

KBM REKOMMENDERAR ■ 2007:2

IT-säkerhetsstandarden Common Criteria (CC) – en introduktion

VAD ÄR CC OCH CCRA?
TILL VAD KAN MAN ANVÄNDA CC?
VAD GÖR KBM OCH FMV?

Titel: IT-säkerhetsstandarden Common Criteria (CC) – en introduktion
Utgiven av Krisberedskapsmyndigheten (KBM)
Omslagsillustration: Jakob Robertsson/AB Typoform
Illustrationer inlaga: Tomas Widlund/AB Typoform

ISSN: 1652-2893
ISBN: 978-91-85797-02-8
KBM:s dnr: 0176/2007
Grafisk form: AB Typoform
Tryck: Edita, Västerås 2007

Skriften kan erhållas kostnadsfritt från
Krisberedskapsmyndigheten, materielförvaltning
E-post: bestallning@krisberedskapsmyndigheten.se

Skriften kan laddas ned från Krisberedskapsmyndighetens webbplats
www.krisberedskapsmyndigheten.se

kbm rekommenderar 2007:2

Innehåll

Förord 5

Inledning 7
Säker information 7
Säkra informationssystem 7
Informationssäkerhet 8

Säkerhet i produkter och system 9
Standardisering 9
Evaluering 9
Certifiering 9
Assuransnivåer 10

Common Criteria 11
Historik 11
Beskrivning 11
Dokumentation 13

Evaluering och certifiering enligt Common Criteria 15
Inledning 15
Processen 15
Evaluering 16
Assuransnivåer 17
Certifiering 17
Kostnader för certifiering 18

Common Criteria Recognition Arrangement 19
Inledning 19
Medlemmar 20
Organisation 21
Samarbete med ISO/IEC 22

Säkerhetspolitiska aspekter **23**
Inledning **23**
Nationell resurs **24**

Sveriges Certifieringsorgan för IT-säkerhet **25**
Bakgrund **25**
FMV/CSEC:s uppgifter **25**
Den nationella certifieringsordningen **26**
Svenska evalueringsföretag **28**

KBM som signatär inom CCRA **29**
KBM som signatär **29**
Kvalificerat medlemskap **29**
Samarbete mellan KBM och FMV/CSEC **30**

Förord

Den statliga Sårbarhets- och säkerhetsutredningen yttrade i en rapport våren 2001:

"En viktig förebyggande och förtroendeskapande åtgärd är att evaluera och certifiera säkerhet i IT-produkter. Utredningen finner det väsentligt att Sverige etablerar ett system för evaluering och certifiering, liksom att Sverige ansluter sig till den internationella överenskommelsen mellan högt utvecklade länder om att ömsesidigt erkänna varandras utfärdade certifikat.

Samhället i allmänhet och totalförsvaret i synnerhet behöver ha en uppfattning om vilken säkerhetsnivå olika IT-produkter har. Därför behövs ett system för evaluering och certifiering av sådana produkter."

Senare kom den statliga Informationssäkerhetsutredningen med ett yttrade i en rapport våren 2005:

"Samhället har, enligt utredningens mening, låg beställarkompetens för informationssäkerhet, vilket utgör ett grundläggande problem. Staten har ett ansvar för att utveckla beställarkompetensen. Tillgång till certifierade produkter enligt Common Criteria eller för tjänster enligt Ledningssystem för informationssäkerhet skulle avsevärt underlätta upphandling av informationssäkerhet."

Som en konsekvens av ovanstående har Försvarets materielverk (FMV) fått regeringens uppdrag att etablera en nationell certifieringsordning för säkerhet i IT-produkter och -system baserat på den internationella IT-säkerhetsstandarden Common Criteria (CC). För detta ändamål har FMV inrättat Sveriges Certifieringsorgan för IT-säkerhet (CSEC).

Regeringen beslutade också år 2006 att Krisberedskapsmyndigheten (KBM) från den 1 januari 2007 ska vara svensk representant – signatär – i Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (CCRA). KBM blev därigenom svensk representant i den internationella

CCRA-organisationen. Även FMV/CSEC ingår i CCRA-samarbetet och ska i egenskap av nationellt certifieringsorgan representera den nationella certifieringsordningen.

Med anledning av dessa aktiviteter har KBM och FMV/CSEC inlett ett nära samarbete kring dessa frågor och har i samverkan utgivit denna skrift. Tanken är att på en grundläggande nivå förklara vad de aktuella begreppen innebär och vad meningen är med det hela. Skriften ska kunna användas vid informationsmöten, kurser och liknande men även kunna användas fristående som en allmän introduktion i ämnet. Kapitlen i skriften är tänkta att kunna läsas fristående från varandra.

Stockholm september 2007

Ingvar Hellquist
Informationssäkerhetsenheten
Krisberedskapsmyndigheten

Dag Ströman
Sveriges Certifieringsorgan
för IT-säkerhet
Försvarets materielverk

Inledning

Säker information

I Regeringens proposition 2005/06:133 Samverkan vid kris – för ett säkrare samhälle, konstaterades att:

"Tillgång till korrekt och säker information vid rätt tillfälle är en förutsättning för trygghet, tillväxt, konkurrens, utveckling och välfärd. Informationstekniken har möjliggjort en explosionsartad utveckling inom informationsförsörjningen.

Sverige har en internationellt framstående ställning i fråga om investeringar i och användning av ny teknik. Ny teknik – där uppgifter och information bearbetas, lagras och förmedlas elektroniskt – innebär emellertid inte bara ökade möjligheter, utan också sårbarheter och beroenden. Tekniken utvecklas ofta snabbare än säkerhetsarbetet.

En rad verksamheter är beroende av en fungerande informationsförsörjning för att kunna upprätthålla produktionen av tjänster och varor. Säker informationsförsörjning är viktig för att uppnå en robusthet i samhällsviktig verksamhet."

Säkra informationssystem

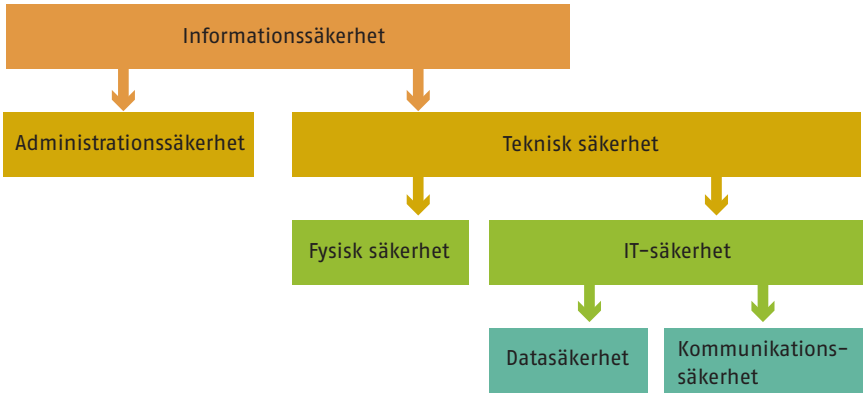
De informationssystem som omger oss blir allt mer komplexa – och framför allt beroende av varandra. Det tydligaste exemplet på detta är det ömsesidiga beroendet mellan el-, tele- och IT-systemen, där ett avbrott i ett av systemen får återverkningar i de andra. Den samhällsviktiga informationsinfrastrukturen är samtidigt en delmängd av övrig samhällsviktig teknisk infrastruktur och påverkar alla sektorer i samhället.

En fortlöpande höjning av säkerheten i informationssystemen är en grundförutsättning för det framtida informationssamhället. All användning av informationsteknik (IT) är nämligen starkt beroende

av att IT-produkter och -system har säkerhetsegenskaper som ger det skydd som krävs och utlovas.

Informationssäkerhet

Enligt den svenska standardiseringsorganisationen SIS handbok 550 Terminologi för informationssäkerhet definieras *informationssäkerhet* som "säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla önskad konfidentialitet, tillförlitlighet och tillgänglighet". Begreppet omfattar såväl IT-säkerhet som säkerhet i administrativa rutiner. Detta illustreras i nedanstående bild:



Informationssäkerhet uppnår man dels genom att införa lämpliga skyddsåtgärder som omfattar riktlinjer, processer och organisation, dels och inte minst genom att använda säkra tekniska produkter som program och maskinvara. Dessa åtgärder måste utformas, genomföras, övervakas, granskas och förbättras för att det ska kunna säkerställas att en organisations säkerhetsmål kan uppnås.

Säkerhet i produkter och system

Standardisering

Enligt den svenska standardiseringsorganisationen SIS är *standardisering* "en verksamhet för att, med hänsyn till aktuella eller tänkbara problem, ta fram beskrivningar för allmän och upprepad tillämpning i syfte att nå största möjliga reda i ett visst sammanhang".

Syftet med standardisering är alltså att förenkla verksamheter i samhället. Det förutsätter därför samarbete och samförstånd mellan företrädare för olika samhällsintressen. Standardiseringen ska tillgodose behov och önskemål från många olika parter och bör så långt som möjligt möta samtligas intressen.

Användning av standarder inom informationssäkerheten är alltså ett sätt att effektivisera säkerhetsarbetet.

Evaluering

Granskning av tekniska säkerhetsegenskaper kallas normalt evaluering. Denna typ av granskning sker oftast av en oberoende, särskilt godkänd part, ett evalueringsföretag. Evalueringen följer en fastställd standard och kraven ställs enligt en standardiserad metod utifrån risker och hot mot produkten eller systemet och dess användning. Syftet med evalueringen är att skapa förtroende.

Certifiering

Resultatet av en evaluering fastställs av ett certifieringsorgan som även har till uppgift att övervaka evalueringsföretagens rutiner, metoder och kompetens. I många länder är certifieringsorganen själva godkända – ackrediterade – av en nationell ackredite-

ringsmyndighet. I Sverige är det nationella ackrediteringsorganet Swedac.

En köpare ska kunna lita på att certifierade produkter och system fyller de ställda och allmänt accepterade kraven. En utvecklare eller leverantör beskriver hur detta ska uppnås genom att fastställa nödvändiga säkerhetsmål. En tredje part – evalueringsföretag – testar och utför säkerhetsvärderingen. Certifieringen utförs av certifieringsorganet och om uppställda krav är uppfyllda kan produkten certifieras.

Assuransnivåer

Evalueringen sker enligt en fastställd standard och kan ske med varierande noggrannhet – utifrån skilda så kallade assuransnivåer – och kan därmed genomföras till varierande kostnad och resultera i olika grad av tillit till produkten. Facktermen för måttet på detta förtroende är *assurans*.

Åtgärder för att skapa assurans kan normalt inte hanteras inom den egna organisationen. Få organisationer har nämligen resurser och kompetens för att kunna bedöma säkerheten i de produkter man avser att använda. Man är här beroende av generella, gemensamma åtgärder. Detta gäller i första hand åtgärder som syftar till att reducera sannolikheten för att det förekommer svagheter som någon kan utnyttja i tekniska lösningar.

Common Criteria

Historik

Tidigt under 80-talet utvecklades i USA Trusted Computer Security Evaluation Criteria (TCSEC), även kallat Orange Book, som omfattade kriterier för försvarets behov inriktade mot det kommersiella utbudet av IT-produkter och -system. Under senare delen av 80-talet utvecklades också evalueringskriterier för IT-säkerhet i flera länder i Europa. Samarbete mellan Storbritannien, Frankrike, Nederländerna och Tyskland resulterade 1991 i gemensamma evalueringskriterier för IT-säkerhet under beteckningen ITSEC. En parallell utveckling i USA och Kanada resulterade i Federal Criteria respektive Canadian Criteria.

De ovan nämnda evalueringskriterierna för IT-säkerhet är nu ersatta av Common Criteria (CC) som är ett resultat av internationellt samarbete inom ramen för samarbetsorganisationen Common Criteria Recognition Arrangement (CCRA), som beskrivs senare i denna skrift, och inom den internationella standardiseringsorganisationen International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). Dessa kriterier har fått standardbeteckningen ISO/IEC 15408. CC version 1.0 fastställdes 1996 och under 2006 fastställdes version 3.1.

Beskrivning

Common Criteria är en standard för hur man ställer krav, deklarerar och evaluerar säkerhet i IT-produkter och -system i deras användningsmiljöer. CC är alltså ett ramverk för hur man beskriver de funktionella kraven på IT-säkerhet i en produkt eller ett system, inte en samling krav i sig. Inom ramverket klarläggs först kravbilden så att produkten eller systemet sedan ska kunna evalueras i förhållande till denna. CC fokuserar på det behov av informations-

säkerhet (konfidentialitet, tillförlitlighet och tillgänglighet) som uppstår på grund av avsiktliga eller oavsiktliga hot.

Inom CC används sju assuransnivåer, Evaluation Assurance Levels (EAL), där EAL 1 är den lägsta nivån och EAL 7 den högsta. Genom assuransnivåerna ges aktörerna ett verktyg för att balansera behovet av tillit till certifierade IT-produkter och -system. Av bilden nedan framgår vad de olika assuransnivåerna ger skydd mot:

Kraven på säkerhet anges i:

- Kravprofiler, Protection Profiles (PP), som beskriver köparens önskemål och krav generellt för en viss typ av produkter, till exempel brandväggar.
- Säkerhetsmål, Security Targets (ST), som beskriver leverantörens utfästelser för en specifik produkt, till exempel en viss brandvägg.

Kraven på säkerhet enligt CC kan ställas utifrån två olika aspekter:

- Funktionskrav – vilka säkerhetsfunktioner behövs för att möta hoten?
- Assuranskrav – hur noggrant bör säkerhetsfunktionerna utvärderas och verifieras?

Dokumentation

Common Criteria omfattar dokumentation i följande delar:

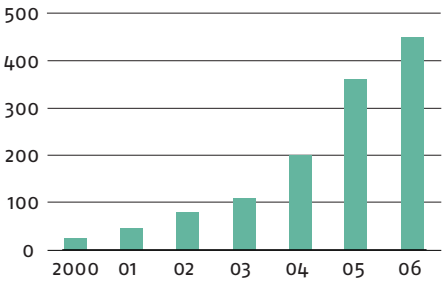
- CC del 1 är en introduktion till metoden, terminologin och aktuella roller. Här beskrivs strukturen och de principer som gäller vid evaluering.
- CC del 2 ger en detaljerad beskrivning av funktionella säkerhetskrav. Här finns en katalog över funktionella säkerhetskomponenter indelade i familjer och klasser.
- CC del 3 listar assuranskrav paketerade i sju olika assuransnivåer. Här finns även evalueringskriterier för kravprofiler och säkerhetsmål.

Dessutom tillkommer:

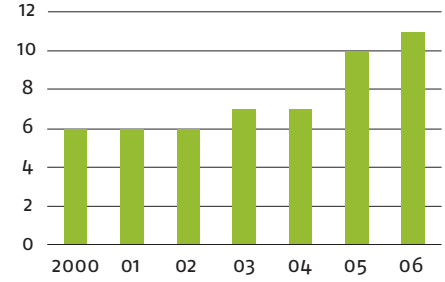
- Common Evaluation Methodology (CEM) (ISO/IEC 18045), som är en standardiserad evalueringsmetodik som i detalj reglerar principerna och stegen i en säkerhetsutvärdering enligt CC.
- ISO/IEC Guide (ISO/IEC TR 15446), som är en guide för utveckling av kravprofiler (PP) och säkerhetsmål (ST). Denna guide är till för utvecklare av PP och ST men kan också ge stöd till certifieringsorgan och evalueringsföretag.

Användningen av CC ökar internationellt

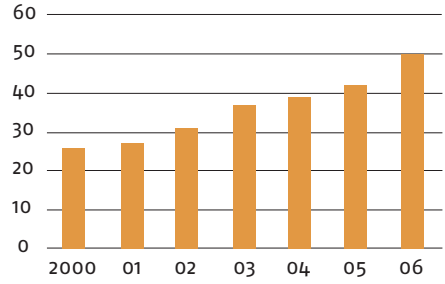
Antalet utfärdade certifikat



Antalet certifieringsordningar



Antalet evalueringsföretag



Evaluering och certifiering enligt Common Criteria

Inledning

Med hjälp av Common Criteria ges upphandlare av IT-produkter och -system möjlighet att ange krav på säkerhetsfunktioner och på säkerhetsgranskning på ett standardiserat och internationellt erkänt sätt. Detta sker genom beskrivning av kraven i kravprofiler. CC ger leverantörer möjlighet att deklarera sina produkters eller systems säkerhetsfunktioner och hur dessa kan granskas i säkerhetsmål.

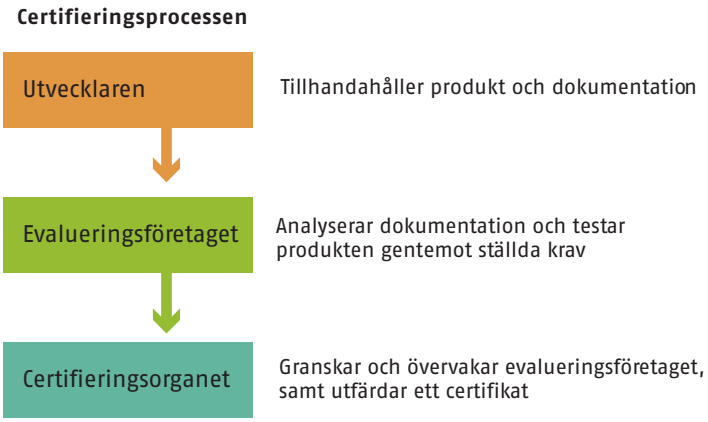
De krav som anger vad som ska granskas i en given IT-produkt eller -system anges i dokument som skrivs enligt den form som anges i CC. Detta gör det möjligt att jämföra olika produkter eller system vid till exempel upphandling.

CC-dokumenten anger hur IT-produkter eller -system fungerar när de sätts i drift samt vilka krav de ställer på omgivningen och administrationen. CC ger även en värdefull vägledning för dem som utvecklar produkter och system som innehåller IT-säkerhetsfunktioner.

Processen

IT-produkter eller -system utvärderas med hjälp av CC enligt en process som kan sammanfattas på följande sätt:

- Leverantören skickar IT-produkten eller -systemet med tillhörande dokumentation till ett licensierat evalueringsföretag.
- Evalueringsförtaget granskar dokumentationen och testar produkten gentemot säkerhetsmålet eller kravprofilen samt skriver en evalueringsrapport.
- Certifieringsorganet övervakar och godkänner evalueringsföretagets arbete och publicerar ett certifikat.



Evaluering

Evalueringsföretaget granskar om de anspråk på IT-produkten eller -systemet som leverantören har angett i säkerhetsmålet eller kravprofilen stämmer med verkligheten. När evalueringsföretaget granskar överensstämmelsen mellan å ena sidan produkt eller system och å andra sidan säkerhetsmål använder den till exempel någon eller några av följande metoder:

- Analys av processer och procedurer vid utveckling av produkt eller system samt kontroll av att processer och procedurer tillämpas.
- Analys av konstruktionsdokument som jämförs med de krav som anges i säkerhetsmålet eller kravprofilen samt analys av korrespondensen mellan olika abstraktionsnivåer i dokumentationen (funktion, högnivådesign, lågnivådesign).
- Verifiering av överensstämmelse mellan lågnivådesign och implementering (till exempel källkod) samt verifiering av matematiska bevis (för till exempel kryptering och hash-algoritmer).
- Analys av funktionella tester och testresultat som har genomförts av leverantören samt analys av användardokumentation.
- Oberoende funktionell testning, genomförd av evalueringsföretaget samt sårbarhetsanalys eller penetrationstest.

Vilka av metoderna ovan som används vid granskning av en specifik IT-produkt eller -system definieras genom vilken assuransnivå som angetts i säkerhetsmålet.

Assuransnivåer

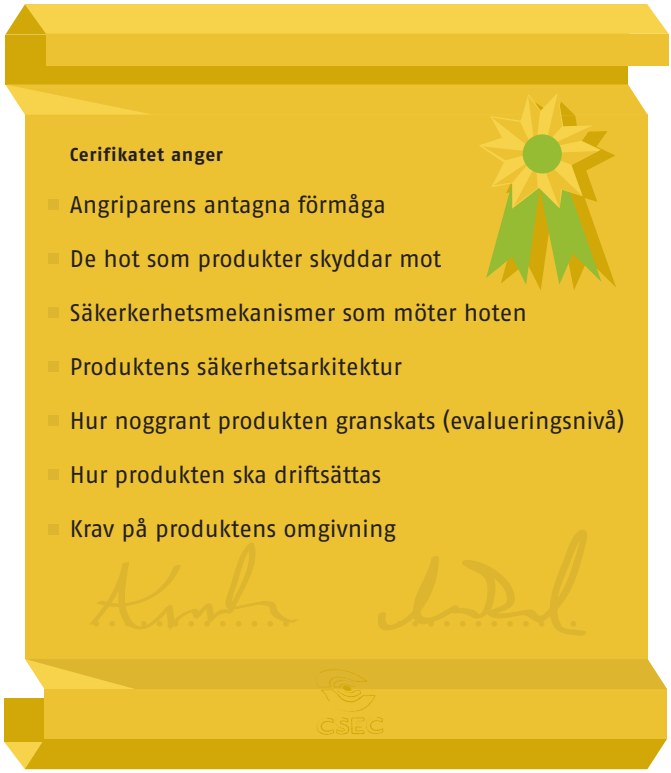
Inom CC används sju assuransnivåer – Evaluation Assurance Level (EAL). Från EAL 1 till och med EAL 4 används i ökande grad metoder som kontrollerar dokumentation, funktionalitet och överensstämmelse med implementationen. Från och med EAL 5 ställs krav på hur produkten blivit konstruerad, för att slutligen vid EAL 7 även omfatta krav på formella bevis på att produkten är framställd enligt specifikationen.

Den valda assuransnivån kan bero på många faktorer som till exempel tillgångarnas skyddsvärde, den driftsmiljö som är aktuell, vilken hotbild som är aktuell, vilken budget som finns tillgänglig och hur benägen man är att ta risker. Genom assuransnivåerna ges aktörerna ett verktyg för att balansera behovet av tillit till IT-produkter och -system mot de kostnader det medför att genomföra en evaluering.

Certifiering

Certifieringsorganet övervakar och godkänner evalueringsföretagets arbete och publicerar ett certifikat. Slutresultatet, certifikatet med tillhörande rapport, anger bland annat:

- En angriparens antagna förmåga att hitta svagheter i produkten eller systemet samt vilka IT-säkerhetsrelaterade hot som förväntas.
- Vilka policier och regler produkten uppfyller, vilka säkerhetsmekanismer som används för att möta hoten samt vilken säkerhetsarkitektur som produkten har.
- Styrkan på säkerhetsmekanismerna samt hur noggrant säkerhetsmekanismerna har granskats och verifierats – assuransnivån.
- Villkor för hur produkten eller systemet på ett säkert sätt ska sättas i drift samt krav på omgivningen för att säkerheten ska upprätthållas.



Kostnader för certifiering

För de allra flesta IT-produkter och -system medför en evaluering på nivå EAL 1 en högst begränsad kostnad men kan ändå ge ett stort värde för systemägaren. Ett certifikat enligt EAL 1 anger tydligt under vilka förutsättningar leverantören avser att produkten eller systemet ska kunna användas säkert och vilken grundläggande testning som gjorts. En evaluering på till exempel EAL 4 medför en större kostnad då denna även omfattar analys av bland annat konstruktionsdokument och källkod. För en mer komplex produkt kan kostnaden uppgå till miljontals kronor.

Ytterligare information:
www.commoncriteriaportal.org
www.csec.se

Common Criteria Recognition Arrangement

Inledning

Sverige är medlem i CCRA som är ett avtal för ömsesidigt erkännande av certifikat utgivna av medlemsnationerna. Den fullständiga uttydningen av CCRA är Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security. CCRA är inte enbart en avtalsstruktur utan också en internationell samarbetsorganisation baserad på ömsesidigt erkännande av utfärdade certifikat.

Ömsesidigt erkännande betyder att nationella certifieringsordningar och de organisationer som har olika roller i dessa uppfyller uppställda krav och dessutom är bedömda och godkända av CCRA. Som ett resultat av detta erkänns utfärdade certifikat av alla övriga CCRA-nationer vid statlig upphandling. Avtalet avser certifieringar upp till assuransnivån EAL 4.

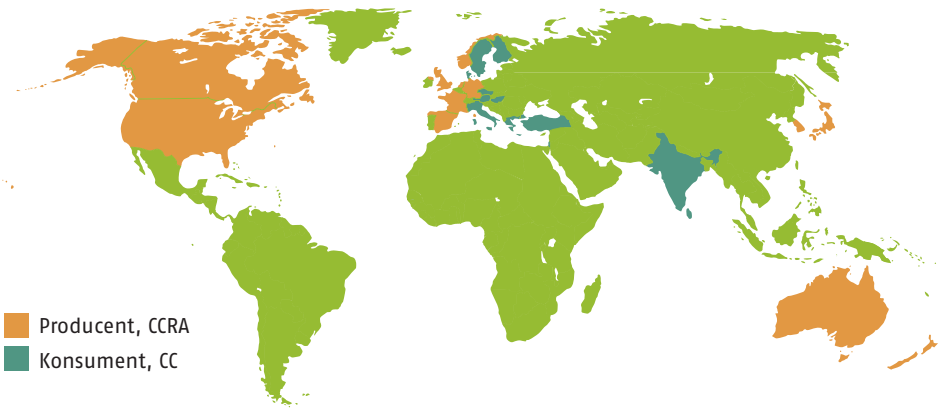
Samarbetet inom CCRA omfattar dessutom att:

- Säkerställa att utvärdering av IT-produkter och -system sker med hög tillförlitlighet och konsistens.
- Öka tillgången på utvärderade IT-produkter och -system samt förbättrade kravprofiler för ökad säkerhet.
- Eliminera behovet av dubblerade granskningar av IT-produkter och -system samt kravprofiler.
- Kontinuerligt utveckla ändamålsenligheten och kostnadseffektiviteten i metodiken för att utvärdera dels IT-produkter och –system, dels kravprofiler.

Medlemmar

I dag (2007) är 24 nationer medlemmar i CCRA. Det finns två typer av medlemskap:

- Producent – Certificate Authorizing Participant – är ett land som har infört en av CCRA erkänd nationell certifieringsordning och som därmed kan utfärda certifikat. I dag är följande länder producenter: Australien, Nya Zeeland, Kanada, Frankrike, Japan, Tyskland, Nederländerna, Norge, Storbritannien, Sydkorea, Spanien och USA.
- Konsument – Certificate Consuming Participant – innebär att landet erkänner CC-certifieringar inom avtalet men inte har någon nationell certifieringsordning och därmed inte certifierar produkter. I dag är följande länder konsumenter: Danmark, Finland, Grekland, Indien, Israel, Italien, Singapore, Sverige, Tjeckien, Turkiet, Ungern och Österrike.



Producentländer erkänner självfallet även de andra ländernas certifikat och är därmed i den meningen även konsumenter.

Sverige är för närvarande (2007) ett konsumentland, men håller på att uppgraderas till producentland.

Organisation

CCRA är alltså även en internationell organisationsstruktur där medlemskapet är baserat på CCRA-avtalet. Inom CCRA-organisationen utvecklas såväl standarden som metoder och regelverk för att stödja avtalet om ömsesidigt erkännande.

Management Committee (MC)

Enligt artikel 10 i CCRA-avtalet ska detta administreras av en Management Committee. Samtliga nationer som undertecknat avtalet har en plats i MC, och kommittén ska sammanträda så ofta det behövs för att förvalta avtalet. I praktiken möts MC endast en gång per år och behandlar då policyfrågor, förslag till ändringar av avtalet, godkännande av nya certifieringsorgan och dylikt. MC kan också tillsätta arbetsgrupper och mellan mötena fatta beslut via e-post.

Executive Subcommittee (ES)

Enligt avtalet ska MC inom sig också tillsätta en Executive Subcommittee som har till uppgift att sköta det löpande arbetet och förse MC med råd och förslag. Verksamhetsinriktningen för ES framgår av CCRA-avtalet, men MC har även utfärdat en instruktion som ytterligare fastställer verksamhetsinriktningen för ES. I ES ingår de producerande CCRA-medlemmarna, det vill säga länder som har infört en av CCRA erkänd nationell certifieringsordning eller är på väg att etablera en egen certifieringsordning. Dessutom tillåts två ytterligare konsumentländer att delta. ES har möte ungefär två gånger per år.

Development Board (DB)

MC har genom en särskilt instruktion fastställt verksamhetsinriktningen för ett Development Board som har till huvuduppgift att vidareutveckla CC och CEM samt att harmonisera de nationella certifieringsordningarna.

Maintenance Board (MB)

Genom en särskilt instruktion har MC även fastställt verksamhetsinriktningen för ett Maintenance Board som har till huvuduppgift att underhålla CC och CEM, huvudsakligen genom att hantera ändringsförslag och ta ställning till förslag till tolkningar.

Samtliga ovanstående kommittéer kan inom sig även tillsätta arbetsgrupper där arbetet leds av en utsedd nation – en så kallad Lead nation – med aktivt deltagande från andra nationer – så kallade Interested nations.

Samarbete med ISO/IEC

Common Criteria har standardbeteckningen ISO/IEC 15408 och Common Evaluation Methodology har beteckningen ISO/IEC 18045. Dessa dokument är alltså internationella standarder. Den huvudsakliga utvecklingen av CC och CEM sker dock inom CCRA:s DB och MB (se ovan) och därefter sker den formella standardiseringen inom organisationen ISO/IEC.

Ytterligare information:
www.commoncriteriaportal.org
www.sis.se

Säkerhetspolitiska aspekter

Inledning

CCRA är en samverkan mellan nationer där det övergripande gemensamma målet är att höja den nationella säkerheten genom att Common Criteria används som ett verktyg för kravställning och granskning. Ett annat gemensamt mål är att verka för att antalet säkra IT-produkter och -system ökar.

Historiskt sett har de myndigheter som utför certifieringar i de ledande industriländerna haft en starkt uttalad önskan att säkerställa kvalitet och objektivitet i de genomförda granskningarna, vid såväl evaluering som certifiering. Denna modell har setts som viktig mot bakgrund av respektive nations egna behov av tillit till IT-säkerheten i de produkter och system som används inom känsliga sektorer som försvar och säkerhet.

Man har av dessa skäl själv tagit den övervakande kvalitetskontrollrollen och inkorporerat denna i certifieringsrollen. De deltagande länderna inspekterar regelbundet verksamheten hos varandras certifieringsorgan genom så kallad Voluntary Periodic Assessment (VPA), för att säkerställa att deltagande länder vidmakthåller kvaliteten i sina certifieringsordningar och tolkar standarden på likvärdigt sätt.

Denna insyn sker genom att varje certifieringsorgan inom CCRA regelbundet granskas på plats av representanter från minst två av de övriga certifikatutgivande länderna. Därefter skrivs en rapport som distribueras till samtliga medlemmar i CCRA. Ett enhälligt beslut krävs sedan för att ett certifieringsorgan ska bli godkänt. Granskningen sker minst en gång vart femte år.

Nationell resurs

De ledande CCRA-ländernas certifieringsorgan är genomgående inrättade inom myndigheter med ansvar för nationellt försvar eller säkerhet. Det ömsesidiga förtroendet baseras härvid i grunden på det mångåriga samarbete som funnits och finns mellan dessa länder. Sverige har genom tidiga insatser, inte minst genom landets aktiva roll i det internationella standardiseringsarbetet kring CC, goda förutsättningar att skapa förtroende för det svenska systemet.

CCRA-avtalet anger som en möjlighet att certifieringsorgan, inom ramen för CC, kan ackrediteras enligt standarden EN 45011 (ISO Guide 65). Alternativt kan organet enligt CCRA-avtalet etableras genom regeringsbeslut eller författning. Motiven för en statlig roll inom området har varit att man ser systemet som en nationell resurs med koppling till nationella säkerhetsintressen. Dessa motiv har förstärkts under senare år med ökade risker för cyber attacker och uppmärksammade svagheter i kritiska infrastrukturer.

Sveriges Certifieringsorgan för IT-säkerhet

Bakgrund

Försvarets materielverk (FMV) har enligt regleringsbrev från regeringen uppdrag att etablera en nationell certifieringsordning för säkerhet i IT-produkter och -system i enlighet med vad regeringen uttalat i propositionen 2001/02:158 Samhällets säkerhet och beredskap.

FMV har vidare uppdraget att verka som nationellt certifieringsorgan för säkerhet i IT-produkter och -system och ska som sådant representera den nationella certifieringsordningen inom CCRA-samarbetet. FMV ska även kunna uppfylla kraven för sådana organ baserat på lagen (1992:1119) om teknisk kontroll så att FMV:s certifieringar i övrigt erkänns inom EU. Uppdraget löstes genom att FMV etablerade Sveriges Certifieringsorgan för IT-säkerhet (CSEC) som en oberoende enhet inom FMV.

Certifieringsorganets officiella namn är Sveriges Certifieringsorgan för IT-säkerhet, dess engelska benämning är Swedish Certification Body for IT Security och dess förkortning är CSEC. FMV/CSEC är en självständig enhet inom FMV med i dag (2007) motsvarande cirka 8 heltidstjänster. Verksamhetens syfte är att säkerställa att säkerhetsfunktioner i certifierade IT-produkter och -system verkligen ger det skydd som utlovas.

FMV/CSEC:s uppgifter

FMV/CSEC ansvarar för utvecklingen och förvaltningen av reglerna för hur Common Criteria tillämpas inom den svenska nationella certifieringsordningen och dess verksamhetsledningssystem, vilket bland annat omfattar regler, processer, avtalsmallar, priser och checklistor.

CSEC har som uppgift att:

- Licensiera evalueringsföretag efter de principer som tillämpas i CCRA samt ge stöd och råd vid utnyttjande av CC för kravspecifikation.
- Utöva tillsyn över de evalueringsföretag som man har knutit till sig vad gäller kompetens och metodik.
- Godkänna nya uppdrag till evalueringsföretag i syfte att säkerställa en rimlig balans mellan ambitionsnivå, IT-produktens eller -systemets komplexitet och bedömd tids- och resursåtgång.
- Följa upp pågående evalueringsuppdrag, granska evalueringsrapporter samt utfärda certifikat.
- Medverka i internationell samverkan i syfte att säkerställa och vidmakthålla erkännande av svenska certifikat samt att effektivisera metodiken för evaluering.

Därutöver ska FMV/CSEC sprida kunskap och information om metoder och procedurer som rör tillämpningen av CC i syfte att öka tilliten till de IT-produkter och -system som används i samhället.

Den nationella certifieringsordningen

Fyra aktörer är involverade i evaluerings- och certifieringsprocessen enligt den svenska certifieringsordningen:

* Utvecklare, det vill säga företag som tillhandahåller IT-produkter eller -system

- Sponsor, det vill säga en organisation som beställer och finansierar oberoende granskning av IT-produkter eller -system
- Evalueringsföretag, som genomför granskning av IT-produkten eller -systemet i enlighet med CC och certifieringsordningen
- Certifieringsorgan, som granskar och godkänner evalueringsföretagets rapporter och utfärdar certifikat.

Avtal om evaluering mellan sponsor och utvecklare

Evaluering och certifiering av IT-produkter eller -system på assuransnivå EAL 2 eller högre kräver medverkan från utvecklaren eftersom evalueringen förutsätter att evalueringsföretaget ges tillgång till teknisk produktdokumentation som utvecklaren äger. Vid granskning av IT-produkter eller -system på assuransnivå EAL 1 sker ingen granskning av sådan dokumentation och sponsorn kan i de flesta fall beställa evalueringen utan medverkan från utvecklaren.

Beställning av evaluering

Sponsorn kontaktar ett evalueringsföretag som ska utföra evalueringen. Tillsammans med evalueringsföretaget producerar sponsorn underlag för ansökan om certifiering med tillhörande underlag.

Beställning av certifiering

När certifieringsansökan med tillhörande underlag är klar skickar sponsorn denna till FMV/CSEC som granskar ansökan och levererar en offert till sponsorn. Utifrån villkoren i offerten kan sponsorn därefter beställa en certifiering.

Produkt: IT-produkt eller -system inkluderande underlag

Utvecklaren (eller sponsorn) levererar IT-produkten eller -systemet till evalueringsföretaget. För EAL 2 eller högre ska utvecklaren även leverera evalueringsunderlag till evalueringsföretaget.

Evalueringsrapporter

Evalueringsföretaget genomför evalueringen genom att utföra de aktiviteter som anges i evalueringsmetodiken och dokumentationen i certifieringsordningen. Resultatet av aktiviteterna dokumenteras och rapporteras till FMV/CSEC.

Granskningsrapporter

FMV/CSEC övervakar genomförandet av evalueringen och utför oberoende granskning av resultat från evalueringen. Resultatet av granskningen och övervakningen rapporteras till evalueringsföretaget för eventuell åtgärd.

Certifikat och certifieringsrapporter

Baserat på den slutliga evalueringsrapporten från evalueringsföretaget producerar FMV/CSEC en certifieringsrapport. Om IT-produkten eller -systemet uppfyller de specificerade kraven, utfärdar certifieringsorganet ett certifikat.

Ytterligare information:
www.csec.se

Svenska evalueringsföretag

Utvärderingen av IT-produkter eller -system enligt CC genomförs av evalueringsföretag – IT Security Evaluation Facility (ITSEF). En evalueringsföretag ska vara licensierad av det nationella certifieringsorganet inom ramen för certifieringsordningen.

FMV/CSEC har i skrivande stund (2007) utfärdat provisoriska licenser (så kallad Provisional License) till två evalueringsföretag. Dessa är Combitech AB och Atsec information security AB. Licenserna har utfärdats efter att organisationernas kvalitets- och säkerhetssystem har granskats och det har säkerställts att företagen har tillräcklig evaluerarkompetens. Licenserna ger företagen rätt att genomföra evalueringar av säkerhet i IT-produkt och -system under överinseende av FMV/CSEC.

Ytterligare information:
www.combitech.se
www.atsec.org

KBM som signatär inom CCRA

KBM som signatär

Regeringen har beslutat att KBM från den 1 januari 2007 ska vara svensk signatär inom CCRA. KBM blev därigenom svensk representant i den internationella CCRA-organisationen. Säkerhetscertifiering enligt Common Criteria och medlemskap i CCRA bedöms som viktigt för Sveriges trovärdighet som avancerad IT-nation.

Att inneha signatärskapet innebär att KBM representerar Sverige i CCRA Management Committee (MC) och den verkställande underkommittén (ES). Dessa kommittéer behandlar frågor som rör själva CCRA-avtalet.

Signatären KBM är även, i CCRA-avtalets mening, sponsor för Sveriges certifieringsorgan för IT-säkerhet – FMV/CSEC – och auktoriserar dess utfärdade CC-certifikat. CSEC representerar Sverige i CCRA:s kommittéer för utveckling och förvaltning (DB och MB) som hanterar frågor av teknisk karaktär rörande CC-standarden samt frågor angående certifieringsordningen.

Ytterligare information:
www.krisberedskapsmyndigheten.se

Kvalificerat medlemskap

CCRA-avtalet anger att enbart signatärer som förfogar över resurserna hos sitt eget lands certifieringsorgan kan nå den högsta medlemsstatusen inom CCRA, nämligen som så kallad Qualified Participant. Det är endast den senare formen av medlemmar som tillåts leda granskningen av andra länders certifieringsorgan eftersom det bara är sådana länder som kan utse representanter med lämplig teknisk kompetens och erfarenhet.

CCRA-avtalet anger också bland annat att

- Signatären ska representera och tillvarata certifieringsorganets intressen inom CCRA-gruppen.
- Signatären ska utse tekniskt kompetenta representanter vid den ömsesidiga granskningen av andra länders certifieringsorgan.
- Varje certifieringsorgan ska etablera och förvalta sin egen certifieringsordning och vidareutveckla systemet samt fastställa tolkningar av kriterierna.
- Certifieringsorganen ska licensiera evalueringsföretag i det egna landet och utöva tillsyn över dessa.

Samarbete mellan KBM och FMV/CSEC

KBM och FMV/CSEC har upprättat riktlinjer för hur samarbetet kring arbete med CC och CCRA ska bedrivas samt hur Sverige ska representeras inom ramen för CCRA. Inom ramen för detta ska bland annat följande gälla:

- Ett nära samarbete mellan parterna ska etableras och regelbundna planerings- och avstämningsmöten ska genomföras i syfte att leva upp till CCRA-avtalets krav för kvalificerat medlemskap (Qualified Participant).
- En rådgivande kommitté – Scheme Advisory Committee (SAC) – ska tillsättas och ha till uppgift att säkerställa oberoendet i FMV/CSEC:s verksamhet samt att möjliggöra för alla relevanta intressenter att delta i utvecklingen av policy och principer för den nationella certifieringsordningen.
- Informationsspridning ska ske via FMV:s hemsida www.commoncriteria.se och via KBM:s hemsida www.krisberedskapsmyndigheten.se samt via informationsskrifter, pressmeddelanden och dylikt.

KBM REKOMMENDERAR

2007:2 IT-säkerhetsstandarden Common Criteria (CC) – en introduktion

2007:1 Kommunens geografiska områdesansvar
Krishanteringsrådets samordnande roll

2006:3 Så vill vi utveckla övningsverksamheten
En strategi för utveckling av generell krishanteringsförmåga i samhället

2006:2 Kommunens övningsverksamhet
Tre enkla sätt att öva kommunledning och förvaltningar i krishantering

2006:1 Basnivå för informationssäkerhet (BITS)
Utgåva 3

2004:1 Kommunens plan för hantering av extraordinära händelser
Vägledning från Krisberedskapsmyndigheten

2003:2 Basnivå för IT-säkerhet (BITS)

2003:1 Risk- och sårbarhetsanalyser
Vägledning för statliga myndigheter

SEMA RECOMMENDS

2003:2 Basic level for IT Security (BITS)

ISSN: 1652-2893
ISBN: 978-91-85797-02-8

Krisberedskapsmyndigheten

Box 599
101 31 Stockholm

Tel 08-593 710 00
Fax 08-593 710 01

kbm@krisberedskaps
myndigheten.se

www.krisberedskaps
myndigheten.se