# Zertifizierung von Sicherheitsprodukten nach Common Criteria

## Besonderheiten für eingebettete Systeme

Jaroslav Svacina, Jaroslav.Svacina@fokus.fraunhofer.de
Nadja Menz, Nadja.Menz@fokus.fraunhofer.de
Thilo Ernst, Thilo.Ernst@fokus.fraunhofer.de

**Die Digitalisierung vieler gesellschaftlicher Bereiche schreitet mit enormer Geschwindigkeit voran. Unzählige Branchen setzen immer mehr auf Digitalisierung von Daten, Automatisierung von Prozessen sowie Vernetzung einzelner Komponenten und Systeme. Neben den entsprechenden Vorteilen bietet die aktuelle Entwicklung jedoch neue vielfältige Angriffspotentiale, welche, wenn richtig ausgenutzt, zu enormen finanziellen oder Personenschäden führen können.**
**Um das Vertrauen in die Sicherheit zu steigern, können Software- und Hardwareprodukte nach ISO/IEC 15408 (Common Criteria) zertifiziert werden. Dieser Beitrag gibt einen Überblick über die Zertifizierung von Sicherheitsprodukten nach Common Criteria und geht dabei gezielt auf einige Besonderheiten im Kontext der eingebetteten Systeme ein.**

### Einleitung

Die zunehmende Digitalisierung und Technologisierung verschiedenster Bereiche bringen viele Vorteile für den Endkunden. So ist es beispielsweise möglich, sein Eigenheim mit dem Smartphone zu steuern, aus dem vernetzten Fahrzeug auf Internetdienste zuzugreifen oder Daten über die ärztliche Behandlung digitalisiert und in der Telematikinfrastruktur des Gesundheitswesens sicher zu verwalten. Der Einsatz neuer, komplexer und vernetzter Technologien bietet jedoch auch zusätzliches Missbrauchspotential durch neue Sicherheitslücken. Die böswillige Ausnutzung solcher Sicherheitslücken führt nicht selten zu erheblichen Schäden.
Ein hohes Sicherheitslevel und das entsprechende Vertrauen in die Sicherheitsprodukte spielen daher sowohl in der Wirtschaft als auch im privaten Bereich eine immer wichtigere Rolle. Gerade der Wunsch nach Vertrauen in IT Sicherheitsprodukte stellt den Kunden vor eine gewaltige Herausforderung. Viele Kunden sind oftmals nicht in der Lage, zu erfassen, welche Sicherheitsfunktionalität ein Produkt bietet und inwieweit es die gewünschten Sicherheitsanforderungen erfüllt. Des Weiteren ist es für den Kunden ohne eine unabhängige Expertenbegutachtung nahezu unmöglich in Erfahrung zu bringen, inwieweit die angegebenen Mechanismen korrekt umgesetzt sind.
Mit den Common Criteria (ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation, kurz CC) [2] wurde ein Standard zur Bewertung und Prüfung von Sicherheitsfunktionalitäten von IT Produkten nach gestaffelten Vertrauenswürdigkeitsstufen geschaffen.

Die Common Criteria bieten Mittel zur Spezifikation der Sicherheitsanforderungen und eine einheitliche Methodik zur Evaluierung und Bewertung der umgesetzten Sicherheitsfunktionalitäten. Im Rahmen spezieller Abkommen ist ein Common Criteria IT-Sicherheitszertifikat international anerkannt und ermöglicht die Gegenüberstellung der Sicherheitseigenschaften zertifizierter Produkte. Ein CC Zertifikat liefert klare Aussagen bezüglich der behaupteten Sicherheitseigenschaften: Korrektheit der Sicherheitsfunktionalität, Wirksamkeit der Sicherheitsfunktionalität gegen Angriffe, Analyse der potentiellen Schwachstellen sowie entsprechende Prüftiefe. Ausgehend von den Sicherheitsvorgaben (Security Target, ST), die dem Zertifikat zugrunde liegen, hat der Abnehmer des zertifizierten Produkts die Möglichkeit, die entsprechende Sicherheitsfunktionalität zu erfassen und zu

entscheiden, inwieweit dieses Produkt für den geplanten Einsatzzweck und die vorgesehene Einsatzumgebung aus sicherheitstechnischer Sicht geeignet ist.

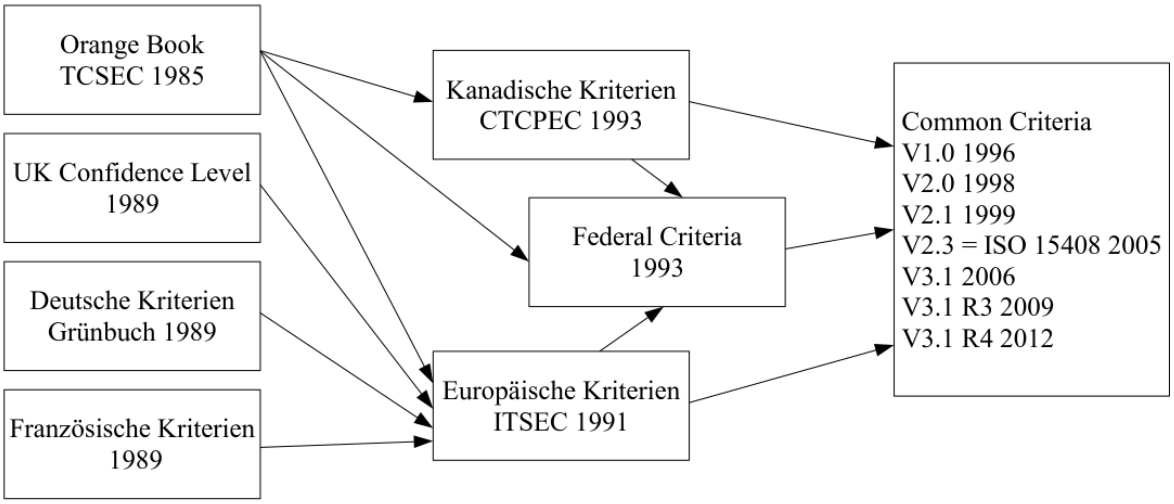


**Abbildung 1: Abhängigkeiten zwischen Kriterienkatalogen [1]**

Abbildung 1 zeigt die Entstehungsgeschichte der Common Criteria. Die ersten Kriterien zur methodischen Bewertung der Sicherheit in der Informationstechnik waren Trusted Computer System Evaluation Criteria (TCSEC) des amerikanischen Verteidigungsministeriums. Im gleichen Zeitraum entstanden in Großbritannien, Deutschland und Frankreich vergleichbare Kriterien, die dann 1991 zusammen mit den TCSEC in die gemeinsamen europäischen Kriterien eingeflossen sind. Mit der voranschreitenden Globalisierung entstand der Wunsch nach einheitlichen und international anerkannten Kriterien, die in Form der Common Criteria entwickelt wurden. Die CC sind eine Weiterentwicklung und Harmonisierung der europäischen ITSEC-Kriterien, der TCSEC bzw. Federal Criteria der USA sowie der kanadischen Kriterien (CTCPEC) [1].

**CC Zertifizierungslandschaft**

Die globalen Ziele der Common Criteria Mitgliedstaaten sind ein gemeinsames standardisiertes Kriterienwerk für IT-Sicherheitsprodukte sowie eine Evaluierungsmethodik, welche die Resultate vergleichbar macht. Diese Vergleichbarkeit bildet die Grundlage für die gegenseitige internationale Anerkennung der Zertifikate.

Die globale Zusammenarbeit findet im Kontext des Common Criteria Recognition Arrangement (CCRA) statt [4]. Auf dieser Ebene gibt es Arbeitsgruppen, welche unter anderem die Weiterentwicklung der Common Criteria und der begleitenden Dokumente forcieren sowie die gegenseitige Begutachtung der jeweiligen nationalen Zertifizierungsschemata organisieren und durchführen. Im Kontext der CCRA gibt es Länder, die ein Zertifikat ausstellen dürfen (z. B. Deutschland, Frankreich, USA) und Länder, die ein Zertifikat nur anerkennen dürfen (z. B. Tschechische Republik, Israel). Das CCRA schließt Zertifizierungen nach international abgestimmten Schutzprofilen (collaborative Protection Profile, cPP) sowie Zertifikate für Vertrauenswürdigkeitskomponenten bis einschließlich der Stufe EAL 2 ein.

Des Weiteren findet eine dedizierte Zusammenarbeit auf europäischer Ebene auf Grundlage des sogenannten SOGIS-MRA (Senior Official Group Information Systems Security – Mutual Recognition Agreement) statt [5]. Auch in diesem Kontext werden die teilnehmenden Länder bzgl. ihrer Rolle klassifiziert. Es gibt einerseits Länder, die Zertifikate ausstellen (und natürlich auch anerkennen) und Länder, die Zertifikate nur anerkennen dürfen. Dies gilt

üblicherweise für Zertifikate bis zur EAL Stufe 4. In bestimmten technischen Domänen werden innerhalb des SOGIS-MRA Zertifikate bis EAL 7 gegenseitig anerkannt. Darüber hinaus sind die SOGIS Arbeitsgruppen bemüht, eine Harmonisierung der Anwendung von CC-Sicherheitskriterien und der Vorgehensweisen in Zertifizierungsverfahren mittels sogenannter Joint Interpretation Library (JIL) Dokumenten voranzutreiben. Diese Interpretationen werden dann in der Regel in das CCRA eingebracht und von der entsprechenden CCRA Arbeitsgruppe (CC Development Board) als sogenannte CC-unterstützende Dokumente verabschiedet.

In den jeweiligen Ländern sind staatliche oder staatlich anerkannte Institutionen für die Zertifizierung nach CC verantwortlich. Die entsprechenden Prozesse und nationalen Charakteristika werden durch die nationalen Zertifizierungsschemata festgelegt. In Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Zertifizierung von Produkten nach Common Criteria verantwortlich. Das BSI begleitet deren Evaluierung, so dass die Vergleichbarkeit der Bewertung sowie ein hohes Vertrauen in die Ergebnisse gewährleistet sind. Die rechtliche Grundlage zur Durchführung von Zertifizierungsverfahren bilden die Zertifizierungsverordnung und das Gesetz zur Stärkung der Sicherheit der Informationstechnik des Bundes. Abbildung 2 zeigt die in Deutschland am Zertifizierungsverfahren beteiligten Parteien, wobei die Beauftragung des CertLab von Fraunhofer FOKUS bei Bedarf durch das BSI erfolgt.

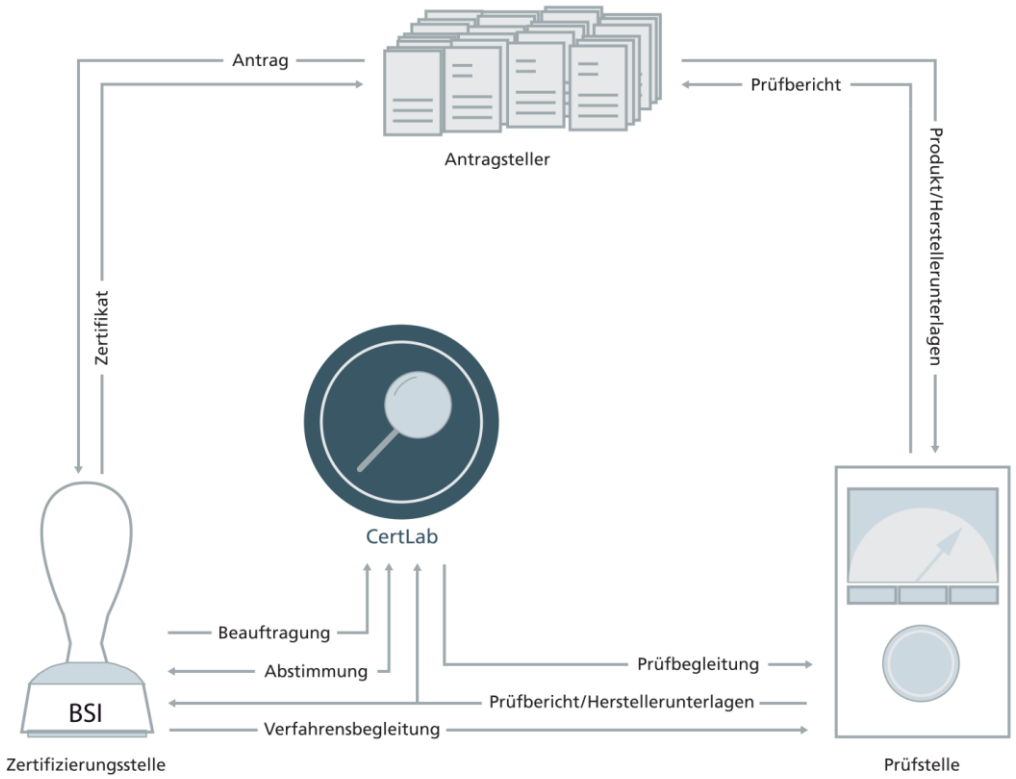


**Abbildung 2: Deutsches Zertifizierungsschema**

Der Prozess beginnt, indem der Produkthersteller einen Zertifizierungsantrag beim BSI stellt. Das BSI begutachtet den Antrag bezüglich grundsätzlicher Zertifizierbarkeit und erteilt im positiven Fall eine Zertifizierungs-ID. Die Evaluierung (Prüfung der Dokumentation, Audit der relevanten Standorte, unabhängige Korrektheitstests und Schwachstellenanalyse mit Penetrationstests) wird von einer unabhängigen Prüfstelle durchgeführt. Die Prüfstelle muss zuvor vom BSI entsprechend akkreditiert worden sein. Die Resultate der einzelnen

Prüfaspekte werden in Form von Prüfberichten dokumentiert. Die Zertifizierungsstelle (BSI) überwacht die Prozesse und stellt eine einheitliche Vorgehensweise sowie die Vergleichbarkeit der Prüfergebnisse sicher. Die Zertifizierungsstelle behält sich vor, konkrete Interpretationen der CC sowie zusätzliche Sicherheitsanforderungen, beispielsweise an Kryptoalgorithmen und Zufallszahlengeneratoren, in die Zertifizierung einfließen zu lassen. Abschließend werden bei positiver Zertifizierungsentscheidung die Prüfberichte abgenommen und das Zertifikat vom BSI ausgestellt.

Nachdem ein Hersteller beim BSI einen Antrag auf Zertifizierung gestellt hat, wird vom BSI bei Bedarf das CertLab im Fraunhofer FOKUS mit der Prüfbegleitung des Verfahrens beauftragt. Ein Mitarbeiter des CertLab übernimmt dabei im Auftrag des BSI große Teile der Prüfbegleitung. Die Verfahrenshoheit und insbesondere die Verantwortung für das Verfahren und das ausgestellte Zertifikat verbleiben zu jeder Zeit beim BSI.

Zu einigen Aspekten geben die Common Criteria keine Auskunft bzw. lassen Interpretationsspielräume offen. Daher publizieren die nationalen Zertifizierungsstellen und Standardisierungsgremien zusätzliche Dokumente, die bestimmte Aspekte präzisieren oder völlig neue Konzepte einführen. Auf CCRA und SOGIS Ebene handelt es sich um die CC Supporting Documents und JIL Dokumente, auf nationaler Ebene sind es die Anwendungshinweise und Interpretationen zum Schema (AIS Dokumente) [6].

**Common Criteria Überblick**

Die Common Criteria verfolgen das Ziel, die Sicherheitsfunktionalität eines Produkts auf Wirksamkeit und Korrektheit auf vergleichbare Art und Weise prüfbar zu machen. Des Weiteren werden die im Produkt enthaltenen und evaluierten Sicherheitsmechanismen durch die CC-Zertifizierung transparent gemacht. Für die Durchführung einer CC-Zertifizierung gibt es mehrere Gründe. Prinzipiell kann jeder Hersteller seine IT-Sicherheitsprodukte zertifizieren lassen. Ein CC-Zertifikat steigert das Vertrauen der Kunden und kann somit für Marketingzwecke eingesetzt werden. Die evaluierten Sicherheitseigenschaften und Sicherheitsfunktionalitäten (inkl. der Prüftiefe) sind nach der Evaluierung in den Sicherheitsvorgaben für das Produkt dokumentiert. Es gibt jedoch Fälle, in denen ein Kunde bzw. ein Auftraggeber eine gewisse Sicherheitsfunktionalität fordert und ohne ein entsprechendes CC-Zertifikat das Produkt nicht für den gewünschten Zweck eingesetzt oder erfolgreich vermarktet werden kann. Beispiele hierfür sind hoheitliche Dokumente (z. B. elektronischer Reisepass) und Komponenten für die Telematikinfrastruktur im Gesundheitswesen. Hier werden die Sicherheitsfunktionalität und die Prüftiefe explizit gefordert (z. B. durch die zuständigen Bundesbehörden). In diesen Situationen kommen sogenannte Schutzprofile (Protection Profile, PP) zum Einsatz, welche die Anforderungen konkret und vereinheitlicht spezifizieren. Möchte also ein Hersteller ein Produkt in einem solchen Marktsegment unterbringen und zertifizieren lassen, ist eine Konformität der Sicherheitsvorgaben zum gewünschten Schutzprofil erforderlich.

Die Common Criteria V3.1R4 bestehen aus vier Teilen: Part 1-3 (ISO/IEC 15408) [2] und CEM, der Common Methodology for Information Technology Security Evaluation (ISO/IEC 18045) [3]. Teil 1 beschreibt die Philosophie, die CC Konzepte und definiert die Begriffswelt. Des Weiteren wird genau spezifiziert, wie die Sicherheitsvorgaben und die Schutzprofile zu gestalten sind. Es wird nicht immer notwendigerweise ein gesamtes Produkt evaluiert. Zur Abgrenzung der zu evaluierenden Sicherheitsfunktionalität wird in Teil 1 der CC das Konzept „Evaluierungsgegenstand“ (Target of Evaluation, TOE) eingeführt. Die Evaluierung umfasst daher nur genau die Sicherheitsfunktionalität, die sich im Kontext des TOEs befindet und für die im ST und/oder PP geeigneten Sicherheitsanforderungen aufgestellt sind. Erst wenn die

Sicherheitsvorgaben stimmig und konsistent sind und der TOE genau definiert ist, kann die eigentliche Evaluierung beginnen.

Teil 2 beschreibt einen Katalog mit Anforderungen an die Sicherheitsfunktionalität (Security Functional Requirements, SFR) des TOEs. Diese Anforderungen sind im ST und PP zu verwenden. Bestimmte Teile der Anforderungen sind nicht spezifiziert und müssen spätestens im ST konkretisiert werden. Die Anforderungen aus Teil 2 spiegeln allgemein anerkanntes und akzeptiertes Expertenwissen wider. Sollten die SFRs in einzelnen Situation nicht ausreichen, können diese erweitert oder neue SFRs nach einem in der CC festgeschriebenen Vorgehen definiert werden. Die SFRs sind in Klassen und Familien mit mindestens einer Komponente strukturiert.

Teil 3 beschreibt eine Sammlung von Anforderungen an die Vertrauenswürdigkeit (Security Assurance Requirements, SAR). Die SARs stellen Anforderungen an den Inhalt der Prüfnachweise sowie an die für die Evaluierung notwendigen Tätigkeiten der Hersteller und Evaluatoren dar. Mit den SARs werden unter anderem der Prüfumfang und die Prüftiefe festgelegt. Daher sind die Anforderungen ebenfalls in das ST/PP aufzunehmen. Die Strukturierung erfolgt ähnlich der Strukturierung der SFRs. Um den Umgang mit SARs zu vereinfachen und eine verständliche Metrik für die Vertrauenswürdigkeit zu geben, werden zudem Vertrauenswürdigkeitskomponenten in Evaluationsstufen für Vertrauenswürdigkeit (Evaluation Assurance Level, EAL) zusammengefasst. Mit steigender Evaluierungsstufe erhöhen sich der Prüfaufwand und die Prüftiefe.

Teil 3 der CC beschreibt in Form von Vertrauenswürdigkeitskomponenten, welche Inhalte (Dokumentation, Tests, Source Code, etc.) geprüft werden und welche Tätigkeiten von den an der Zertifizierung beteiligten Entwicklern und Evaluatoren grob erwartet werden. Die CEM verfeinert die Aktivitäten der Evaluatoren und gibt eine methodische Anleitung für die Durchführung. Nur eine einheitliche Evaluierungsmethodik ermöglicht die Anerkennung der Zertifikate im Rahmen bestimmter Abkommen. Als Beispiel sei hier die Familie AVA_VAN (Vulnerability Assessment) genannt. Teil 3 besagt, dass im Rahmen dieser Familie eine Schwachstelleanalyse je nach konkreter Komponente mit unterschiedlichem Umfang und unterschiedlicher Tiefe durchgeführt werden muss. Die CEM unterteilt die jeweilige Komponente in einzelne detaillierte Arbeitsanweisungen (Work Units, WU) und gibt methodische Hinweise. So wird beispielsweise das Angriffspotential für die Ausnutzung einer potentiellen Schwachstelle klassifiziert (Basic, Enhanced-Basic, Moderate und High). Des Weiteren bietet die CEM einen Mechanismus zur Bewertung einer potentiellen Schwachstelle hinsichtlich des für das Ausnutzen benötigten Angriffspotentials. Basierend auf der Analyse der potentiellen Schwachstellen, der durchgeführten Penetrationstests und der anschließenden Bewertung kann systematisch hergeleitet werden, welche Angreifer mit welchem Angriffspotential der TOE abwehren kann. Informationen zu konkreten Angriffen kann die CEM aufgrund der Vielfalt der Produkte nicht bieten. Im Rahmen vom SOGIS-MRA werden jedoch in speziellen technischen Domänen konkrete Angriffe auf bestimmte Produkttypen untersucht und als unterstützende Dokumente herausgegeben.

**Besonderheiten der CC für eingebettete Systeme**

Im Rahmen der CC werden sowohl Software- als auch Hardwareprodukte zertifiziert. Vertreter reiner Softwareprodukte sind beispielsweise Firewalls und Desktop/Server Betriebssysteme. Ein häufiger Produkttyp im Hardwarebereich ist die Smartcard mit hohen Anforderungen an die Sicherheit. Dieser Produkttyp kommt in vielfältigen Bereichen zur Anwendung. Aufgrund der vielen domänenspezifischen Besonderheiten der jeweiligen Produkttypen werden im SOGIS-MRA Kontext sogenannte technische Domänen definiert.

Bisher sind es „Smartcards and Similar Devices“ und „Hardware Devices with Security Boxes”. Innerhalb der technischen Domänen werden für diese Bereiche spezifische Interpretationen der CC sowie weitere unterstützende Dokumente herausgegeben, welche zum Teil bei der entsprechenden CC Zertifizierung verbindlich zu berücksichtigen sind. Nachfolgend werden einige Besonderheiten der technischen Domäne „Smartcards and Similar Devices“ vorgestellt:

*Composite Evaluation:*
Die Sicherheitschips (Basis für die Smartcard Produkte) werden üblicherweise zusammen mit unterschiedlichen Betriebssystemen und Anwendungen eingesetzt. Würden nun im Rahmen einer jeden Zertifizierung die Anwendung, das Betriebssystem und die Hardwareplattform (Sicherheitschip inkl. der Firmware) einer kompletten Zertifizierung unterzogen, so müsste die Hardwareplattform jedes Mal erneut evaluiert werden. Daher bedarf es einer zusammengesetzten Evaluierung und Zertifizierung. Die CC bieten einen Kompositionsmechanismus in Form der Vertrauenswürdigkeitsklasse ACO. Dieser Mechanismus adressiert eine zusammengesetzte Evaluierung bestehend aus bereits zertifizierten Komponenten. Dieser Ansatz ist für den Smartcard Bereich jedoch nicht geeignet, da in dieser technischen Domäne die Anforderung besteht, eine nicht zertifizierte Anwendung in Kombination mit einer zertifizierten Plattform zu betrachten. Hierzu haben sich die SOGIS Partner auf den Ansatz „Composite Product Evaluation“ geeinigt [9]. Abbildung 3 vergleicht die beiden Ansätze „ACO“ und „Composite Product Evaluation“.

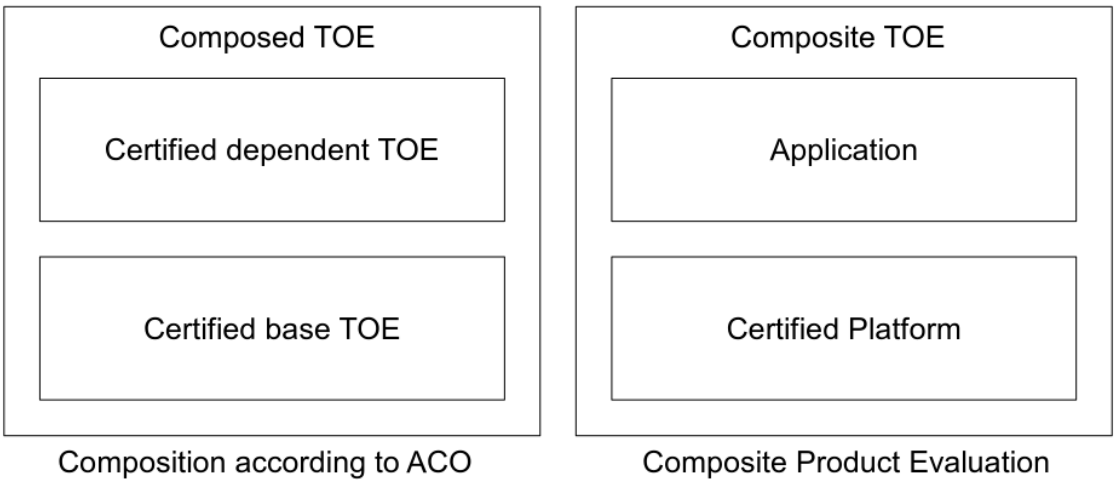


**Abbildung 3: Vergleich der Ansätze zur zusammengesetzten Zertifizierung [9]**

Der Ansatz Composite Product Evaluation ermöglicht eine vertikale Integration zertifizierter Subsysteme im Rahmen einer Zertifizierung des Gesamtsystems. Die unterstützenden Dokumente liefern neben dem generellen Ansatz ebenfalls eine konkrete Erweiterung der Methodik. Viele der bereits existierenden Prüfaspekte wurden in diesem Kontext erweitert (Prüfung der Kompatibilität auf ST Ebene, Berücksichtigung der Auflagen zu Verwendung der Plattform, Integrationstests, etc.). Um einen TOE als Plattform für weitere Zertifizierungen nutzen zu können, muss im Rahmen der Plattformzertifizierung ein zusätzlicher Prüfbericht erstellt werden: Evaluation Technical Report for Composition. Dieses Dokument bildet die Grundlage für die auf der bereits zertifizierten Plattform aufbauende Zertifizierung.

*Berechnung des Angriffspotentials im Smartcard Bereich*
Smartcard Produkte müssen üblicherweise immer einem Angreifer mit hohem Angriffspotential widerstehen. Die in der CEM beschriebene Methodik zur Berechnung des

Angriffspotentials für das erfolgreiche Ausnutzen einer potentiellen Schwachstelle hat sich in dieser technischen Domäne als unzureichend herausgestellt. Die JHAS Gruppe (JIL Hardware Attacks Subgroup) hat daher einen an die Domäne angepassten Ansatz definiert [8]. Eine der Haupterweiterungen besteht aus der Separierung der Angriffsphasen. So werden die Phasen „Identification“ und „Exploitation“ eines Angriffs separat betrachtet und bewertet. Die Phase „Identification“ bezieht sich auf den Aufwand, der notwendig ist, einen Angriff zu entdecken und seine Machbarkeit zu demonstrieren. Die Phase „Exploitation“ betrachtet den Aufwand für die tatsächliche Durchführung des Angriffs. Erst die gemeinsame Betrachtung dieser Phasen liefert die Gesamtsichtweise auf das für den Angriff notwendige Angriffspotential. Auch die Betrachtung sogenannter „Open Samples“ (Exemplare des Produkts mit eingeschränkten Sicherheitsmechanismen oder bekannten Geheimnissen) fließt in die Berechnung des Angriffspotentials ein.

*Anforderungen an die Produktions- und Entwicklungsstandorte*
Unabhängig von der für die Zertifizierung des Smartcard Produkts verwendeten EAL Stufe (meistens EAL4 und höher) werden üblicherweise noch folgende SAR Komponenten hinzugezogen (Augmentierung der EAL Stufe): AVA_VAN.5 – Resistenz gegen Angreifer mit hohem Angriffspotential und ALC_DVS.2 – Hohe Sicherheit der Entwicklungs- und Produktionsumgebungen, geeignet für Zertifizierungen nach AVA_VAN.5. Für solche Zertifizierungen ist die Anwendung des Dokuments „Minimum Site Security Requirements“ [7] verbindlich. Dieses Dokument beschreibt die Anforderungen an die Entwicklungs- und Produktionsstandorte. Neben Anforderung an die Dokumentation der Nachweise werden konkrete Vorgaben bzgl. relevanter Aspekte, wie Organisation der Informations- und Datensicherheit, Asset-Management, Personalsicherheit, physische und umgebungsbezogene Sicherheit, Kommunikation und Betriebsabläufe sowie Management der Zugriffskontrolle gegeben.

**Verlässlichkeit und Nachhaltigkeit der Zertifizierung**
Für den Nutzer bzw. Kunden ist es essenziell zu wissen, in welchem Maße er Zusicherungen über die Sicherheit eines Produktes tatsächlich vertrauen kann. Die Common Criteria verfolgen daher das Ziel, dem Nutzer je nach EAL-Stufe eine dem Sicherheitsbedarf angepasste Menge von Belegen für die Vertrauenswürdigkeit des Produkts an die Hand zu geben. Diese Belege zeigen, welche Maßnahmen bei Entwicklung und Realisierung des Produkts getroffen wurden, um das Produkt sicher zu machen. Die so belegte Vertrauenswürdigkeit ist natürlich an verschiedene Bedingungen gebunden. Beispielsweise muss der Nutzer stets in der Lage sein, zu identifizieren, ob er tatsächlich das zertifizierte Produkt (in der zertifizierten Version) in der Hand hat. Auch Handbücher, Datenblätter und andere „Guidance-Dokumente“ werden im Rahmen der Common Criteria evaluiert. Dadurch wird sichergestellt, dass dem Nutzer alle nötigen Informationen zur Verfügung stehen, um das Produkt sachgemäß und vor allem ohne (sonst evtl. selbst verursachte) Sicherheitsbeeinträchtigungen einsetzen zu können.

Die CC berücksichtigen auch die zukünftige Weiterentwicklung zertifizierter Produkte sowie die parallel stattfindende Evolution von Bedrohungen und Angriffstechniken. Wenn im Rahmen einer Produktweiterentwicklung sicherheitsrelevante Änderungen vorgenommen wurden, wird eine Re-Zertifizierung erforderlich. Bei wesentlichen Änderungen der Bedrohungslage wird analog ein Re-Assessment durchgeführt. Hersteller sind weiterhin verpflichtet, der Zertifizierungsstelle neu bekannt gewordene Angriffe auf zertifizierte Produkte mitzuteilen. Darüber hinaus ist generell der Gültigkeitszeitraum eines CC-Zertifikats stets zeitlich beschränkt.

Zur Sicherheitsbewertung werden häufig vertrauliche Informationen des Herstellers benötigt, die nicht einer breiteren Öffentlichkeit bekannt werden sollen. Die Vertraulichkeit solcher Informationen ist verlässlich über den gesamten Prozess einer CC-Zertifizierung gesichert: Nur ein kleiner Personenkreis bei der Zertifizierungsbehörde und der Prüfstelle erhält Zugriff auf vertrauliche Produktinformationen. Besonders sensitives Material wird nur vor Ort beim Hersteller kurzzeitig eingesehen.
Der Hersteller entscheidet auch, ob der Zertifizierungsbericht veröffentlicht wird, und welche Informationen darin enthalten sein dürfen. Für die Sicherheitsvorgaben besteht die Möglichkeit einer Veröffentlichung in reduzierter Form („ST-light“). Bei zertifizierten Plattformen, die als Basis einer späteren Composite-Evaluierung vorgesehen sind, kann ein reduzierter Prüfbericht zur Verwendung im Kompositionsverfahren erstellt werden („ETR for Composition“). Dabei handelt es sich um ein nicht-öffentliches Dokument, das jedoch zur Weitergabe an Beteiligte des Kompositionsverfahrens vorgesehen ist.

**Trends und aktuelle Entwicklungen**

Gerade im Embedded-Bereich gewinnt die IT-Sicherheit aktuell und in naher Zukunft weiter an Bedeutung. Der in verschiedenen Branchen (Automotive, eHealth, Smart Energy und weitere) aufkommende Trend zur Verschiebung der Nachfrage in Richtung vertrauenswürdiger Komponenten kann durch Common Criteria-Zertifizierung hervorragend unterstützt werden. Es ist davon auszugehen, dass dieser Trend insbesondere für Zulieferer in den nächsten Jahren immer mehr an Relevanz gewinnt. Umso wichtiger ist es, die Zusammenarbeit der jeweiligen Zertifizierungsschemata zu forcieren und weiterhin einen gemeinsamen internationalen Kurs zu verfolgen. Die Fortentwicklung von nationalen Protection Profiles hin zu collaborative Protection Profiles zeigt das gemeinsame Bestreben der Nationen im CCRA auf, die kontinuierliche gegenseitige Anerkennung von Zertifikaten zu sichern. Die cPP-Entwicklung wird von international Technical Communities (iTC) vorangetrieben. Die iTC umfassen alle relevanten Interessengruppen wie Produkthersteller, Endkunden, Zertifizierungsstellen und Prüfstellen.

**Zusammenfassung**

Die Zertifizierung nach Common Criteria sorgt für die Einhaltung bestimmter Standards bei der Realisierung von Sicherheitsfunktionalitäten sowie bei der Verwendung von Kryptographie in IT Sicherheitsprodukten. Die Zertifizierung erfordert offenkundig einen gewissen Aufwand, schafft jedoch einheitliche Sicherheitsmaßstäbe im wachsenden Markt für sichere Hardware- sowie Softwareprodukte. Die CC-Standards sind ein offenes Framework, das flexibel auf verschiedenste Anwendungsfälle und Kosten/Nutzen-Szenarien anwendbar ist und ständig weiterentwickelt wird. Die teilnehmenden Länder arbeiten im Kontext der CCRA- und SOGIS-Abkommen sowohl an Konkretisierungen der CC für bestimmte technische Domänen als auch an der Optimierung der CC-Prozesse und Evaluierungstätigkeiten. Dadurch wird sichergestellt, dass die aktuellen technologischen, organisatorischen und prozesstechnischen Entwicklungen adäquat in den Common Criteria berücksichtigt werden.

**Literatur**

[1] Eckert, Claudia: IT-Sicherheit. Oldenburg, 2006
[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.
Part 1: Introduction and general model.
Part 2: Functional security components.
Part 3: Assurance security components.

[3] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.
[4] About The Common Criteria. https://www.commoncriteriaportal.org/ccra/ (Oktober 2015)
[5] SOGIS – Senior Officials Group Information Systems Security. http://www.sogis.org/ (Oktober 2015)
[6] BSI: Anwendungshinweise und Interpretationen (AIS). https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/AnwendungshinweiseundInterpretationen/AIS/AIS.html (Oktober 2015)
[7] JIL: Minimum Site Security Requirements, Version 1.1 (for trial use), July 2013
[8] JIL: Application of Attack Potential to Smartcards, Version 2.9, January 2013
[9] JIL: Composite product evaluation for Smart Cards and similar devices, Version 1.4, August 2015

**Autoren**

**Jaroslav Svacina**
Jaroslav Svacina ist bei Fraunhofer FOKUS als Wissenschaftler und Projektleiter im Bereich der eingebetteten sicherheitskritischen Systeme mit hohen Zertifizierungsanforderungen tätig. Sein Wissen hat er über einen Zeitraum von 3 Jahren aktiv in die AUTOSAR Standardisierung eingebracht. Im Kontext des Fraunhofer FOKUS CertLab begleitet er aktuell für das Bundesamt für Sicherheit in der Informationstechnik Zertifizierungsverfahren nach Common Criteria im Bereich Hardware.

**Nadja Menz**
Nadja Menz arbeitet als wissenschaftliche Mitarbeiterin im Kompetenzzentrum Digital Public Services am Fraunhofer-Institut FOKUS. Sie ist Expertin im Bereich IT-Sicherheit, mit einem Schwerpunkt auf Qualitätssicherung und Zertifizierung. Nadja Menz arbeitet im CertLab, das Zertifizierungen von IT-Sicherheitsprodukten basierend auf dem Common Criteria Standard unter Aufsicht des BSI begleitet. Das CertLab ist deutschlandweit die einzige Instanz, die vom BSI mit dieser vertrauensvollen Aufgabe betraut ist.

**Thilo Ernst**
Thilo Ernst, Senior Scientist am Kompetenzzentrum Digital Public Services des Fraunhofer-Instituts für Offene Kommunikationssysteme, hat in einer breiten Palette von Forschungs- und Entwicklungsvorhaben in Bereichen wie e-Science, Grid/Cloud-Computing, Verkehrstelematik und Embedded Software verschiedenste Facetten des Themas IT-Sicherheit kennengelernt und bringt seine Erfahrungen aktuell in die Begleitung von CC-Zertifizierungsverfahren im Auftrag des BSI ein.