

**DIN EN ISO/IEC 15408-3**

ICS 35.030

Ersatz für  
die 2011-03 zurückgezogene  
Norm  
DIN ISO/IEC 15408-3:2007-11

**Informationstechnik –  
IT-Sicherheitsverfahren –  
Evaluationskriterien für IT-Sicherheit –  
Teil 3: Komponenten zur Sicherheitskontrolle  
(ISO/IEC 15408-3:2008, korrigierte Fassung 2011-06-01);  
Deutsche Fassung EN ISO/IEC 15408-3:2020, nur auf CD-ROM**

Information technology –  
Security techniques –  
Evaluation criteria for IT security –  
Part 3: Security assurance components  
(ISO/IEC 15408-3:2008, Corrected version 2011-06-01);  
German version EN ISO/IEC 15408-3:2020, only on CD-ROM

Technologies de l'information –  
Techniques de sécurité –  
Critères d'évaluation pour la sécurité TI –  
Partie 3: Composants d'assurance de sécurité  
(ISO/IEC 15408-3:2008, Version corrigée 2011-06-01);  
Version allemande EN ISO/IEC 15408-3:2020, seulement en CD-ROM

Gesamtumfang 207 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

## Nationales Vorwort

Der Text von ISO/IEC 15408-3, korrigierte Fassung 2011-06-01 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 15408-3:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Arbeitskreis NA 043-01-27-03 AK „Evaluationskriterien für IT-Sicherheit“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

|                      |       |                                |
|----------------------|-------|--------------------------------|
| ISO/IEC 15408-1:2009 | siehe | DIN EN ISO/IEC 15408-1:2020-12 |
| ISO/IEC 15408-2      | siehe | DIN EN ISO/IEC 15408-2         |

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN ([www.din.de](http://www.din.de)) durch eine Suche nach der Dokumentennummer aufgerufen werden.

## Änderungen

Gegenüber der 2011-03 zurückgezogenen Norm DIN ISO/IEC 15408-3:2007-11 wurden folgende Änderungen vorgenommen:

- a) redaktionelle Überarbeitung, insbesondere bezogen auf ADV\_FSP, ADV\_TDS, ATE\_DPT.2, ATE\_IND und ALC;
- b) Aktualisierung des technischen Inhalts.

## Frühere Ausgaben

DIN ISO/IEC 15408-3: 2001-03, 2007-11

## Nationaler Anhang NA (informativ)

## Literaturhinweise

DIN EN ISO/IEC 15408-1:2020-12, *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 1: Einführung und allgemeines Modell*

DIN EN ISO/IEC 15408-2, *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 2: Sicherheitsfunktionskomponenten*

Deutsche Fassung

Informationstechnik —  
IT-Sicherheitsverfahren —  
Evaluationskriterien für IT-Sicherheit —  
Teil 3: Komponenten zur Sicherheitskontrolle  
(ISO/IEC 15408-3:2008, korrigierte Fassung 2011-06-01)

Information technology —  
Security techniques —  
Evaluation criteria for IT security —  
Part 3: Security assurance components  
(ISO/IEC 15408-3:2008, Corrected version 2011-06-01)

Technologies de l'information —  
Techniques de sécurité —  
Critères d'évaluation pour la sécurité TI —  
Partie 3: Composants d'assurance de sécurité  
(ISO/IEC 15408-3:2008, Version corrigée 2011-06-01)

Diese Europäische Norm wurde vom CEN am 2. März 2020 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN und CENELEC-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



CEN-CENELEC Management-Zentrum:  
Rue de la Science 23, B-1040 Brüssel

## Inhalt

|                                                                                    | Seite |
|------------------------------------------------------------------------------------|-------|
| Europäisches Vorwort .....                                                         | 9     |
| Vorwort .....                                                                      | 10    |
| Einleitung .....                                                                   | 12    |
| 1 Anwendungsbereich .....                                                          | 13    |
| 2 Normative Verweisungen .....                                                     | 13    |
| 3 Begriffe, Symbole und Abkürzungen .....                                          | 13    |
| 4 Übersicht .....                                                                  | 13    |
| 4.1 Aufbau dieses Teils von ISO/IEC 15408 .....                                    | 13    |
| 5 Paradigma für Vertrauenswürdigkeit .....                                         | 14    |
| 5.1 Philosophie von ISO/IEC 15408 .....                                            | 14    |
| 5.2 Ansatz für Vertrauenswürdigkeit .....                                          | 14    |
| 5.2.1 Bedeutung von Anfälligkeiten .....                                           | 14    |
| 5.2.2 Ursachen von Anfälligkeiten .....                                            | 15    |
| 5.2.3 ISO/IEC 15408 Vertrauenswürdigkeit .....                                     | 15    |
| 5.2.4 Vertrauenswürdigkeit durch Evaluierung .....                                 | 15    |
| 5.3 ISO/IEC 15408 Vertrauenswürdigkeitsskala .....                                 | 16    |
| 6 Vertrauenswürdigkeitskomponenten .....                                           | 16    |
| 6.1 Aufbau der Vertrauenswürdigkeitsklassen, -familien und -komponenten .....      | 16    |
| 6.1.1 Struktur der Vertrauenswürdigkeitsklassen .....                              | 16    |
| 6.1.2 Struktur der Vertrauenswürdigkeitsfamilien .....                             | 17    |
| 6.1.3 Struktur der Vertrauenswürdigkeitskomponenten .....                          | 18    |
| 6.1.4 Vertrauenswürdigkeitselemente .....                                          | 20    |
| 6.1.5 Komponententaxonomie .....                                                   | 20    |
| 6.2 Struktur der EAL-Stufen .....                                                  | 21    |
| 6.2.1 Name der EAL-Stufe .....                                                     | 21    |
| 6.2.2 Ziele .....                                                                  | 21    |
| 6.2.3 Anwendungshinweise .....                                                     | 21    |
| 6.2.4 Vertrauenswürdigkeitskomponenten .....                                       | 22    |
| 6.2.5 Beziehung zwischen Vertrauenswürdigkeit und Vertrauenswürdigkeitsstufe ..... | 22    |
| 6.3 Struktur der CAPs .....                                                        | 23    |
| 6.3.1 Name des CAPs .....                                                          | 23    |
| 6.3.2 Ziele .....                                                                  | 23    |
| 6.3.3 Anwendungshinweise .....                                                     | 23    |
| 6.3.4 Vertrauenswürdigkeitskomponenten .....                                       | 24    |
| 6.3.5 Beziehung zwischen Vertrauenswürdigkeit und Vertrauenswürdigkeitsstufe ..... | 24    |
| 7 Vertrauenswürdigkeitsstufen .....                                                | 25    |
| 7.1 Übersicht über die Vertrauenswürdigkeitsstufen (EAL-Stufen) .....              | 25    |
| 7.2 Einzelheiten der Vertrauenswürdigkeitsstufen .....                             | 27    |
| 7.3 Vertrauenswürdigkeitsstufe 1 (EAL1) – funktional geprüft .....                 | 27    |
| 7.3.1 Ziele .....                                                                  | 27    |
| 7.3.2 Vertrauenswürdigkeitskomponenten .....                                       | 27    |
| 7.4 Vertrauenswürdigkeitsstufe 2 (EAL2) – strukturell geprüft .....                | 28    |
| 7.4.1 Ziele .....                                                                  | 28    |
| 7.4.2 Vertrauenswürdigkeitskomponenten .....                                       | 28    |

|        |                                                                                                        |    |
|--------|--------------------------------------------------------------------------------------------------------|----|
| 7.5    | Vertrauenswürdigkeitsstufe 3 (EAL3) – methodisch geprüft und überprüft.....                            | 29 |
| 7.5.1  | Ziele .....                                                                                            | 29 |
| 7.5.2  | Vertrauenswürdigkeitskomponenten.....                                                                  | 29 |
| 7.6    | Vertrauenswürdigkeitsstufe 4 (EAL4) – methodisch entwickelt, geprüft und überprüft .....               | 31 |
| 7.6.1  | Ziele .....                                                                                            | 31 |
| 7.6.2  | Vertrauenswürdigkeitskomponenten.....                                                                  | 31 |
| 7.7    | Vertrauenswürdigkeitsstufe 5 (EAL5) – semiformal entwickelt und geprüft .....                          | 32 |
| 7.7.1  | Ziele .....                                                                                            | 32 |
| 7.7.2  | Vertrauenswürdigkeitskomponenten.....                                                                  | 32 |
| 7.8    | Vertrauenswürdigkeitsstufe 6 (EAL6) – semiformal verifiziertes Design und geprüft.....                 | 33 |
| 7.8.1  | Ziele .....                                                                                            | 33 |
| 7.8.2  | Vertrauenswürdigkeitskomponenten.....                                                                  | 34 |
| 7.9    | Vertrauenswürdigkeitsstufe 7 (EAL7) – formal verifiziertes Design und geprüft.....                     | 35 |
| 7.9.1  | Ziele .....                                                                                            | 35 |
| 7.9.2  | Vertrauenswürdigkeitskomponenten.....                                                                  | 35 |
| 8      | Zusammengesetzte Sicherheitspakete.....                                                                | 36 |
| 8.1    | Übersicht über die zusammengesetzten Sicherheitspakete (CAPs).....                                     | 37 |
| 8.2    | Einzelheiten zusammengesetzter Sicherheitspakete .....                                                 | 38 |
| 8.3    | Zusammengesetztes Sicherheitspaket A (CAP-A) – strukturell zusammengesetzt .....                       | 38 |
| 8.3.1  | Ziele .....                                                                                            | 38 |
| 8.3.2  | Vertrauenswürdigkeitskomponenten.....                                                                  | 39 |
| 8.4    | Zusammengesetztes Sicherheitspaket B (CAP-B) – methodisch zusammengesetzt.....                         | 39 |
| 8.4.1  | Ziele .....                                                                                            | 39 |
| 8.4.2  | Vertrauenswürdigkeitskomponenten.....                                                                  | 40 |
| 8.5    | Zusammengesetztes Sicherheitspaket C (CAP-C) – methodisch zusammengesetzt, geprüft und überprüft ..... | 41 |
| 8.5.1  | Ziele .....                                                                                            | 41 |
| 8.5.2  | Vertrauenswürdigkeitskomponenten.....                                                                  | 41 |
| 9      | Klasse APE: Evaluierung des Schutzprofils.....                                                         | 42 |
| 9.1    | PP-Einleitung (APE_INT).....                                                                           | 43 |
| 9.1.1  | Ziele .....                                                                                            | 43 |
| 9.1.2  | APE_INT.1 PP-Einleitung.....                                                                           | 43 |
| 9.2    | Konformitätsansprüche (APE_CCL) .....                                                                  | 44 |
| 9.2.1  | Ziele .....                                                                                            | 44 |
| 9.2.2  | APE_CCL.1 Konformitätsansprüche .....                                                                  | 44 |
| 9.3    | Sicherheitsproblemdefinition (APE_SPD) .....                                                           | 46 |
| 9.3.1  | Ziele .....                                                                                            | 46 |
| 9.3.2  | APE_SPD.1 Sicherheitsproblemdefinition .....                                                           | 46 |
| 9.4    | Sicherheitszielsetzungen (APE_OBJ) .....                                                               | 47 |
| 9.4.1  | Ziele .....                                                                                            | 47 |
| 9.4.2  | Komponentenebenen.....                                                                                 | 47 |
| 9.4.3  | APE_OBJ.1 Sicherheitszielsetzungen für die Betriebsumgebung.....                                       | 47 |
| 9.4.4  | APE_OBJ.2 Sicherheitszielsetzungen .....                                                               | 47 |
| 9.5    | Erweiterte Komponentendefinition (APE_ECD).....                                                        | 48 |
| 9.5.1  | Ziele .....                                                                                            | 48 |
| 9.5.2  | APE_ECD.1 Erweiterte Komponentendefinition.....                                                        | 49 |
| 9.6    | Sicherheitsanforderungen (APE_REQ) .....                                                               | 50 |
| 9.6.1  | Ziele .....                                                                                            | 50 |
| 9.6.2  | Komponentenebenen.....                                                                                 | 50 |
| 9.6.3  | APE_REQ.1 Festgelegte Sicherheitsanforderungen.....                                                    | 50 |
| 9.6.4  | APE_REQ.2 Abgeleitete Sicherheitsanforderungen .....                                                   | 51 |
| 10     | Klasse ASE: Evaluierung der Sicherheitsvorgabe.....                                                    | 52 |
| 10.1   | ST-Einleitung (ASE_INT).....                                                                           | 53 |
| 10.1.1 | Ziele .....                                                                                            | 53 |

|        |                                                                                                           |    |
|--------|-----------------------------------------------------------------------------------------------------------|----|
| 10.1.2 | ASE_INT.1 ST-Einleitung.....                                                                              | 53 |
| 10.2   | Konformitätsansprüche (ASE_CCL).....                                                                      | 54 |
| 10.2.1 | Ziele .....                                                                                               | 54 |
| 10.2.2 | ASE_CCL.1 Konformitätsansprüche.....                                                                      | 54 |
| 10.3   | Sicherheitsproblemdefinition (ASE_SPD).....                                                               | 56 |
| 10.3.1 | Ziele .....                                                                                               | 56 |
| 10.3.2 | ASE_SPD.1 Sicherheitsproblemdefinition.....                                                               | 56 |
| 10.4   | Sicherheitszielsetzungen (ASE_OBJ).....                                                                   | 57 |
| 10.4.1 | Ziele .....                                                                                               | 57 |
| 10.4.2 | Komponentenebenen.....                                                                                    | 57 |
| 10.4.3 | ASE_OBJ.1 Sicherheitszielsetzungen für die Betriebsumgebung.....                                          | 57 |
| 10.4.4 | ASE_OBJ.2 Sicherheitszielsetzungen.....                                                                   | 57 |
| 10.5   | Erweiterte Komponentendefinition (ASE_ECD) .....                                                          | 59 |
| 10.5.1 | Ziele .....                                                                                               | 59 |
| 10.5.2 | ASE_ECD.1 Erweiterte Komponentendefinition .....                                                          | 59 |
| 10.6   | Sicherheitsanforderungen (ASE_REQ).....                                                                   | 60 |
| 10.6.1 | Ziele .....                                                                                               | 60 |
| 10.6.2 | Komponentenebenen.....                                                                                    | 60 |
| 10.6.3 | ASE_REQ.1 Festgelegte Sicherheitsanforderungen .....                                                      | 60 |
| 10.6.4 | ASE_REQ.2 Abgeleitete Sicherheitsanforderungen .....                                                      | 61 |
| 10.7   | Zusammenfassende Spezifikation des TOEs (ASE_TSS).....                                                    | 62 |
| 10.7.1 | Ziele .....                                                                                               | 62 |
| 10.7.2 | Komponentenebenen.....                                                                                    | 62 |
| 10.7.3 | ASE_TSS.1 Zusammenfassende Spezifikation des TOEs .....                                                   | 63 |
| 10.7.4 | ASE_TSS.2 Zusammenfassende Spezifikation des TOEs mit zusammenfassendem<br>Architekturdesign .....        | 63 |
| 11     | Klasse ADV: Entwicklung.....                                                                              | 64 |
| 11.1   | Sicherheitsarchitektur (ADV_ARC) .....                                                                    | 69 |
| 11.1.1 | Ziele .....                                                                                               | 69 |
| 11.1.2 | Komponentenebenen.....                                                                                    | 69 |
| 11.1.3 | Anwendungshinweise .....                                                                                  | 70 |
| 11.1.4 | ADV_ARC.1 Beschreibung der Sicherheitsarchitektur.....                                                    | 70 |
| 11.2   | Funktionsspezifikation (ADV_FSP) .....                                                                    | 71 |
| 11.2.1 | Ziele .....                                                                                               | 71 |
| 11.2.2 | Komponentenebenen.....                                                                                    | 72 |
| 11.2.3 | Anwendungshinweise .....                                                                                  | 72 |
| 11.2.4 | ADV_FSP.1 Grundlegende Funktionsanforderungen.....                                                        | 75 |
| 11.2.5 | ADV_FSP.2 Sicherheit durchsetzende Funktionsspezifikation .....                                           | 75 |
| 11.2.6 | ADV_FSP.3 Funktionsspezifikation mit vollständiger Zusammenfassung .....                                  | 76 |
| 11.2.7 | ADV_FSP.4 Vollständige Funktionsspezifikation .....                                                       | 78 |
| 11.2.8 | ADV_FSP.5 Vollständige semiformale Funktionsspezifikation mit zusätzlichen<br>Fehlerinformationen.....    | 79 |
| 11.2.9 | ADV_FSP.6 Vollständige semiformale Funktionsspezifikation mit zusätzlicher formaler<br>Spezifikation..... | 80 |
| 11.3   | Darstellung der Implementierung (ADV_IMP).....                                                            | 81 |
| 11.3.1 | Ziele .....                                                                                               | 81 |
| 11.3.2 | Komponentenebenen.....                                                                                    | 82 |
| 11.3.3 | Anwendungshinweise .....                                                                                  | 82 |
| 11.3.4 | ADV_IMP.1 Darstellung der Implementierung der TSF .....                                                   | 83 |
| 11.3.5 | ADV_IMP.2 Vollständige Zuordnung der Darstellung der Implementierung der TSF .....                        | 84 |
| 11.4   | TSF-Interna (ADV_INT) .....                                                                               | 84 |
| 11.4.1 | Ziele .....                                                                                               | 84 |
| 11.4.2 | Komponentenebenen.....                                                                                    | 85 |
| 11.4.3 | Anwendungshinweise .....                                                                                  | 85 |
| 11.4.4 | ADV_INT.1 Wohlstrukturierte Teilmengen von TSF-Interna .....                                              | 85 |

|        |                                                                                                            |     |
|--------|------------------------------------------------------------------------------------------------------------|-----|
| 11.4.5 | ADV_INT.2 Wohlstrukturierte Interna .....                                                                  | 86  |
| 11.4.6 | ADV_INT.3 Minimal komplexe Interna .....                                                                   | 87  |
| 11.5   | Modellierung der Sicherheitspolitik (ADV_SPM).....                                                         | 88  |
| 11.5.1 | Ziele .....                                                                                                | 88  |
| 11.5.2 | Komponentenebenen.....                                                                                     | 89  |
| 11.5.3 | Anwendungshinweise.....                                                                                    | 89  |
| 11.5.4 | ADV_SPM.1 Formales TOE-Sicherheitspolitikmodell.....                                                       | 90  |
| 11.6   | TOE-Design (ADV_TDS) .....                                                                                 | 91  |
| 11.6.1 | Ziele .....                                                                                                | 91  |
| 11.6.2 | Komponentenebenen.....                                                                                     | 91  |
| 11.6.3 | Anwendungshinweise.....                                                                                    | 91  |
| 11.6.4 | ADV_TDS.1 Grundsätzliches Design.....                                                                      | 92  |
| 11.6.5 | ADV_TDS.2 Architekturdesign .....                                                                          | 94  |
| 11.6.6 | ADV_TDS.3 Grundsätzliches modulares Design .....                                                           | 95  |
| 11.6.7 | ADV_TDS.4 Semiformales modulares Design .....                                                              | 96  |
| 11.6.8 | ADV_TDS.5 Vollständiges semiformales modulares Design .....                                                | 98  |
| 11.6.9 | ADV_TDS.6 Vollständiges semiformales modulares Design mit formaler allgemeiner<br>Design Darstellung ..... | 99  |
| 12     | Klasse AGD: Leitliniendokumente.....                                                                       | 100 |
| 12.1   | Operative Leitlinien für Benutzer (AGD_OPE) .....                                                          | 101 |
| 12.1.1 | Ziele .....                                                                                                | 101 |
| 12.1.2 | Komponentenebenen.....                                                                                     | 101 |
| 12.1.3 | Anwendungshinweise.....                                                                                    | 101 |
| 12.1.4 | AGD_OPE.1 Operative Leitlinien für Benutzer .....                                                          | 102 |
| 12.2   | Vorbereitende Verfahren (AGD_PRE) .....                                                                    | 103 |
| 12.2.1 | Ziele .....                                                                                                | 103 |
| 12.2.2 | Komponentenebenen.....                                                                                     | 103 |
| 12.2.3 | Anwendungshinweise.....                                                                                    | 103 |
| 12.2.4 | AGD_PRE.1 Vorbereitende Verfahren .....                                                                    | 104 |
| 13     | Klasse ALC: Unterstützung des Lebenszyklus.....                                                            | 104 |
| 13.1   | CM-Funktionen (ALC_CMC) .....                                                                              | 105 |
| 13.1.1 | Ziele .....                                                                                                | 105 |
| 13.1.2 | Komponentenebenen.....                                                                                     | 106 |
| 13.1.3 | Anwendungshinweise.....                                                                                    | 106 |
| 13.1.4 | ALC_CMC.1 Kennzeichnung des TOEs.....                                                                      | 107 |
| 13.1.5 | ALC_CMC.2 Verwendung eines CM-Systems.....                                                                 | 107 |
| 13.1.6 | ALC_CMC.3 Autorisierungskontrollen.....                                                                    | 108 |
| 13.1.7 | ALC_CMC.4 Herstellungsunterstützung, Abnahmeverfahren und Automatisierung.....                             | 110 |
| 13.1.8 | ALC_CMC.5 Erweiterte Unterstützung.....                                                                    | 112 |
| 13.2   | CM-Umfang (ALC_CMS) .....                                                                                  | 115 |
| 13.2.1 | Ziele .....                                                                                                | 115 |
| 13.2.2 | Komponentenebenen.....                                                                                     | 115 |
| 13.2.3 | Anwendungshinweise.....                                                                                    | 115 |
| 13.2.4 | ALC_CMS.1 CM-Abdeckung des TOEs .....                                                                      | 115 |
| 13.2.5 | ALC_CMS.2 CM-Abdeckung für Teile des TOEs .....                                                            | 116 |
| 13.2.6 | ALC_CMS.3 CM-Abdeckung für die Darstellung der Implementierung .....                                       | 117 |
| 13.2.7 | ALC_CMS.4 CM-Abdeckung für die Problemverfolgung.....                                                      | 118 |
| 13.2.8 | ALC_CMS.5 CM-Abdeckung für Entwicklungswerkzeuge .....                                                     | 118 |
| 13.3   | Lieferung (ALC_DEL).....                                                                                   | 120 |
| 13.3.1 | Ziele .....                                                                                                | 120 |
| 13.3.2 | Komponentenebenen.....                                                                                     | 120 |
| 13.3.3 | Anwendungshinweise.....                                                                                    | 120 |
| 13.3.4 | ALC_DEL.1 Lieferverfahren .....                                                                            | 120 |
| 13.4   | Entwicklungssicherheit (ALC_DVS).....                                                                      | 121 |

|        |                                                                       |     |
|--------|-----------------------------------------------------------------------|-----|
| 13.4.1 | Ziele .....                                                           | 121 |
| 13.4.2 | Komponentenebenen.....                                                | 121 |
| 13.4.3 | Anwendungshinweise .....                                              | 121 |
| 13.4.4 | ALC_DVS.1 Identifikation von Sicherheitsmaßnahmen.....                | 122 |
| 13.4.5 | ALC_DVS.2 Angemessenheit von Sicherheitsmaßnahmen .....               | 122 |
| 13.5   | Mängelbeseitigung (ALC_FLR).....                                      | 123 |
| 13.5.1 | Ziele .....                                                           | 123 |
| 13.5.2 | Komponentenebenen.....                                                | 123 |
| 13.5.3 | Anwendungshinweise .....                                              | 123 |
| 13.5.4 | ALC_FLR.1 Grundlegende Mängelbeseitigung.....                         | 124 |
| 13.5.5 | ALC_FLR.2 Verfahren zu Mängelberichten .....                          | 124 |
| 13.5.6 | ALC_FLR.3 Systematische Mängelbeseitigung.....                        | 126 |
| 13.6   | Definition des Lebenszyklus (ALC_LCD).....                            | 128 |
| 13.6.1 | Ziele .....                                                           | 128 |
| 13.6.2 | Komponentenebenen.....                                                | 128 |
| 13.6.3 | Anwendungshinweise.....                                               | 128 |
| 13.6.4 | ALC_LCD.1 Vom Entwickler definiertes Lebenszyklusmodell.....          | 129 |
| 13.6.5 | ALC_LCD.2 Messbares Lebenszyklusmodell.....                           | 129 |
| 13.7   | Werkzeuge und Techniken (ALC_TAT) .....                               | 130 |
| 13.7.1 | Ziele .....                                                           | 130 |
| 13.7.2 | Komponentenebenen.....                                                | 130 |
| 13.7.3 | Anwendungshinweise .....                                              | 130 |
| 13.7.4 | ALC_TAT.1 Genau festgelegte Entwicklungswerkzeuge .....               | 131 |
| 13.7.5 | ALC_TAT.2 Konformität mit Implementierungsstandards .....             | 131 |
| 13.7.6 | ALC_TAT.3 Konformität mit Implementierungsstandards – alle Teile..... | 132 |
| 14     | Klasse ATE: Prüfungen.....                                            | 133 |
| 14.1   | Abdeckung (ATE_COV).....                                              | 134 |
| 14.1.1 | Ziele .....                                                           | 134 |
| 14.1.2 | Komponentenebenen.....                                                | 134 |
| 14.1.3 | Anwendungshinweise .....                                              | 134 |
| 14.1.4 | ATE_COV.1 Nachweis der Abdeckung.....                                 | 134 |
| 14.1.5 | ATE_COV.2 Analyse der Abdeckung.....                                  | 135 |
| 14.1.6 | ATE_COV.3 Strenge Analyse der Abdeckung.....                          | 136 |
| 14.2   | Tiefe (ATE_DPT).....                                                  | 136 |
| 14.2.1 | Ziele .....                                                           | 136 |
| 14.2.2 | Komponentenebenen.....                                                | 137 |
| 14.2.3 | Anwendungshinweise.....                                               | 137 |
| 14.2.4 | ATE_DPT.1 Prüfung: grundlegendes Design .....                         | 137 |
| 14.2.5 | ATE_DPT.2 Prüfung: sicherheit-durchsetzende Module .....              | 138 |
| 14.2.6 | ATE_DPT.3 Prüfung: modulares Design .....                             | 139 |
| 14.2.7 | ATE_DPT.4 Prüfung: Darstellung der Implementierung.....               | 139 |
| 14.3   | Funktionsprüfungen (ATE_FUN).....                                     | 140 |
| 14.3.1 | Ziele .....                                                           | 140 |
| 14.3.2 | Komponentenebenen.....                                                | 141 |
| 14.3.3 | Anwendungshinweise .....                                              | 141 |
| 14.3.4 | ATE_FUN.1 Funktionsprüfung.....                                       | 141 |
| 14.3.5 | ATE_FUN.2 Geordnete Funktionsprüfungen.....                           | 142 |
| 14.4   | Unabhängiges Prüfen (ATE_IND) .....                                   | 143 |
| 14.4.1 | Ziele .....                                                           | 143 |
| 14.4.2 | Komponentenebenen.....                                                | 143 |
| 14.4.3 | Anwendungshinweise .....                                              | 143 |
| 14.4.4 | ATE_IND.1 Unabhängige Prüfungen – Konformität.....                    | 144 |
| 14.4.5 | ATE_IND.2 Unabhängige Prüfungen – Stichprobe.....                     | 145 |
| 14.4.6 | ATE_IND.3 Unabhängige Prüfungen – vollständig.....                    | 146 |

|                       |                                                                             |     |
|-----------------------|-----------------------------------------------------------------------------|-----|
| 15                    | Klasse AVA: Anfälligkeitsbewertung .....                                    | 147 |
| 15.1                  | Anwendungshinweise.....                                                     | 147 |
| 15.2                  | Anfälligkeitsanalyse (AVA_VAN).....                                         | 148 |
| 15.2.1                | Ziele .....                                                                 | 148 |
| 15.2.2                | Komponentenebenen.....                                                      | 148 |
| 15.2.3                | AVA_VAN.1 Anfälligkeitsuntersuchung .....                                   | 148 |
| 15.2.4                | AVA_VAN.2 Anfälligkeitsanalyse .....                                        | 149 |
| 15.2.5                | AVA_VAN.3 Konzentrierte Anfälligkeitsanalyse.....                           | 150 |
| 15.2.6                | AVA_VAN.4 Methodische Anfälligkeitsanalyse .....                            | 151 |
| 15.2.7                | AVA_VAN.5 Erweiterte methodische Anfälligkeitsanalyse.....                  | 152 |
| 16                    | Klasse ACO: Zusammensetzung.....                                            | 153 |
| 16.1                  | Begründung der Zusammensetzung (ACO_COR).....                               | 156 |
| 16.1.1                | Ziele .....                                                                 | 156 |
| 16.1.2                | Komponentenebenen.....                                                      | 156 |
| 16.1.3                | ACO_COR.1 Begründung der Zusammensetzung.....                               | 156 |
| 16.2                  | Entwicklungsnachweis (ACO_DEV) .....                                        | 157 |
| 16.2.1                | Ziele .....                                                                 | 157 |
| 16.2.2                | Komponentenebenen.....                                                      | 157 |
| 16.2.3                | Anwendungshinweise.....                                                     | 157 |
| 16.2.4                | ACO_DEV.1 Funktionsbeschreibung .....                                       | 158 |
| 16.2.5                | ACO_DEV.2 Einfacher Nachweis des Designs .....                              | 158 |
| 16.2.6                | ACO_DEV.3 Detaillierter Nachweis des Designs .....                          | 159 |
| 16.3                  | Verlässlichkeit der abhängigen Komponente (ACO_REL) .....                   | 160 |
| 16.3.1                | Ziele .....                                                                 | 160 |
| 16.3.2                | Komponentenebenen.....                                                      | 161 |
| 16.3.3                | Anwendungshinweise.....                                                     | 161 |
| 16.3.4                | ACO_REL.1 Einfache Verlässlichkeitsinformation .....                        | 161 |
| 16.3.5                | ACO_REL.2 Verlässlichkeitsinformation .....                                 | 162 |
| 16.4                  | Prüfen des zusammengesetzten TOEs (ACO_CTT) .....                           | 163 |
| 16.4.1                | Ziele .....                                                                 | 163 |
| 16.4.2                | Komponentenebenen.....                                                      | 163 |
| 16.4.3                | Anwendungshinweise.....                                                     | 163 |
| 16.4.4                | ACO_CTT.1 Schnittstellenprüfung .....                                       | 163 |
| 16.4.5                | ACO_CTT.2 Strenge Schnittstellenprüfung.....                                | 165 |
| 16.5                  | Anfälligkeitsanalyse der Zusammensetzung (ACO_VUL).....                     | 166 |
| 16.5.1                | Ziele .....                                                                 | 166 |
| 16.5.2                | Komponentenebenen.....                                                      | 166 |
| 16.5.3                | Anwendungshinweise.....                                                     | 166 |
| 16.5.4                | ACO_VUL.1 Anfälligkeitsüberprüfung der Zusammensetzung .....                | 167 |
| 16.5.5                | ACO_VUL.2 Anfälligkeitsanalyse der Zusammensetzung.....                     | 167 |
| 16.5.6                | ACO_VUL.3 Erweitert-einfache Anfälligkeitsanalyse der Zusammensetzung ..... | 168 |
| Anhang A (informativ) | Entwicklung (ADV).....                                                      | 170 |
| A.1                   | Ergänzende Informationen zu ADV_ARC: Sicherheitsarchitekturen.....          | 170 |
| A.1.1                 | Sicherheitsarchitektureigenschaften .....                                   | 170 |
| A.1.2                 | Sicherheitsarchitekturbeschreibungen .....                                  | 171 |
| A.2                   | ADV_FSP: Ergänzende Informationen zu TSFIs .....                            | 173 |
| A.2.1                 | Bestimmen der TSFI .....                                                    | 174 |
| A.2.2                 | Beispiel: Ein komplexes DBMS .....                                          | 176 |
| A.2.3                 | Beispiel-Funktionsspezifikation.....                                        | 178 |
| A.3                   | ADV_INT: Ergänzende Informationen zu TSF-Interna .....                      | 179 |
| A.3.1                 | Struktur von prozeduraler Software.....                                     | 180 |
| A.3.2                 | Komplexität von prozeduraler Software .....                                 | 182 |
| A.4                   | ADV_TDS: Teilsysteme und Module .....                                       | 182 |
| A.4.1                 | Teilsysteme.....                                                            | 182 |

|                                                                                                   |                                                                                           |     |
|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|-----|
| A.4.2                                                                                             | Module .....                                                                              | 183 |
| A.4.3                                                                                             | Ansatz zur Einstufung .....                                                               | 186 |
| A.5                                                                                               | Ergänzende Informationen zu formalen Methoden.....                                        | 188 |
| Anhang B (informativ) Zusammensetzung (ACO) .....                                                 |                                                                                           | 190 |
| B.1                                                                                               | Notwendigkeit für Evaluierungen zusammengesetzter TOEs .....                              | 190 |
| B.2                                                                                               | Durchführung der Evaluierung von Sicherheitsvorgaben für einen zusammengesetzten TOE..... | 192 |
| B.3                                                                                               | Interaktionen zwischen zusammengesetzten IT-Entitäten .....                               | 192 |
| Anhang C (informativ) Querverweisung von Abhängigkeiten der Vertrauenswürdigkeitskomponenten..... |                                                                                           | 198 |
| Anhang D (informativ) Querverweisung von PPs und Vertrauenswürdigkeitskomponenten.....            |                                                                                           | 203 |
| Anhang E (informativ) Querverweisung von EAL-Stufen und Vertrauenswürdigkeitskomponenten.....     |                                                                                           | 204 |
| Anhang F (informativ) Querverweisung von CAPs und Vertrauenswürdigkeitskomponenten.....           |                                                                                           | 205 |

## Europäisches Vorwort

Der Text von ISO/IEC 15408-3:2008, korrigierte Fassung 2011-06-01 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 15408-3:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis September 2020, und etwaige entgegenstehende nationale Normen müssen bis September 2020 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

### Anerkennungsnotiz

Der Text von ISO/IEC 15408-3:2008, korrigierte Fassung 2011-06-01 wurde von CEN als EN ISO/IEC 15408-3:2020 ohne irgendeine Abänderung genehmigt.

## Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

Internationale Normen werden in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet.

Die Hauptaufgabe der gemeinsamen Technischen Komitees besteht in dem Erarbeiten von internationalen Normen. Die von den Technischen Komitees angenommenen Norm-Entwürfe werden den Mitgliedsorganisationen zur Umfrage zur Verfügung gestellt. Für eine Veröffentlichung als Internationale Norm wird eine Zustimmung von mindestens 75 % der Mitgliedsländer, die abgestimmt haben, benötigt.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

ISO/IEC 15408-3 wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security technique*, erarbeitet. Der identische Text von ISO/IEC 15408 ist bei den am Common Criteria Project beteiligten Organisationen als Common Criteria for Information Technology Security Evaluation (Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik) veröffentlicht. Die einheitliche XML-Quelle für beide Veröffentlichungen finden Sie unter <http://www.oc.ccn.cni.es/xml>.

Diese dritte Fassung ersetzt die zweite Fassung von (ISO/IEC 15408-3:2005), die technisch überarbeitet wurde.

ISO 15408 besteht unter dem allgemeinen Titel *Information technology — Security techniques — Evaluation criteria for IT security* aus den folgenden Teilen:

- *Part 1: Introduction and general model*
- *Part 2: Security functional components*
- *Part 3: Security assurance components*

Diese korrigierte Version von ISO/IEC 15408-3:2008 enthält verschiedene redaktionelle Korrekturen, die sich im Wesentlichen auf die Vertrauenswürdigkeitskomponenten EAL4 und EAL6 sowie ADV\_FSP, ADV\_TDS, ATE\_DPT.2, ATE\_IND und ALC beziehen.

## Rechtlicher Hinweis

Die unten aufgeführten Regierungsorganisationen haben zu der Entwicklung dieser Version der Common Criteria for Information Technology Security Evaluations beigetragen. Als gemeinsame Urheberrechtsinhaber an den Common Criteria for Information Technology Security Evaluations, Version 3.1 Teile 1 bis 3 (kurz CC 3.1), erteilen sie hiermit der ISO/IEC die nicht-exklusive Lizenz zur Verwendung der CC 3.1 für die weitere Entwicklung/Pflege der internationalen Norm ISO/IEC 15408. Diese Regierungsorganisationen behalten sich allerdings das Recht zur Nutzung, Vervielfältigung, zum Vertrieb sowie zur Übersetzung und Änderung der CC 3.1 nach Belieben vor.

|                         |                                                                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------|
| Australien/Neuseeland:  | The Defence Signals Directorate and the Government Communications Security Bureau respectively; |
| Kanada:                 | Communications Security Establishment;                                                          |
| Frankreich:             | Direction Centrale de la Sécurité des Systèmes d'Information;                                   |
| Deutschland:            | Bundesamt für Sicherheit in der Informationstechnik;                                            |
| Japan:                  | Information Technology Promotion Agency;                                                        |
| Niederlande:            | Netherlands National Communications Security Agency;                                            |
| Spanien:                | Ministerio de Administraciones Públicas and Centro Criptológico Nacional;                       |
| Vereinigtes Königreich: | Communications-Electronic Security Group;                                                       |
| USA:                    | The National Security Agency and the National Institute of Standards and Technology.            |

## **Einleitung**

Die in diesem Teil von ISO/IEC 15408 definierten Vertrauenswürdigkeitskomponenten sind die Grundlage für in Schutzprofilen (PPs) oder Sicherheitsvorgaben (STs) ausgedrückten Vertrauenswürdigkeitsanforderungen.

Diese Anforderungen schaffen eine einheitliche Methode zur Formulierung von Vertrauenswürdigkeitsanforderungen für TOEs. Dieser Teil von ISO/IEC 15408 katalogisiert den Satz an Vertrauenswürdigkeitskomponenten, -familien und -klassen. Dieser Teil von ISO/IEC 15408 definiert außerdem die Evaluierungskriterien für PPs und STs und zeigt Vertrauenswürdigkeitsstufen, die die vordefinierte ISO/IEC 15408-Skala zur Bewertung der Vertrauenswürdigkeit von Evaluierungsgegenständen (TOEs) festlegen, die als Vertrauenswürdigkeitsstufen (EAL-Stufen, en: Evaluation Assurance Levels) bezeichnet werden.

Die Zielgruppe für diesen Teil von ISO/IEC 15408 schließt Verbraucher, Entwickler und Evaluatoren von sicheren IT-Produkten ein. ISO/IEC 15408-1:2009, Abschnitt 5, enthält zusätzliche Informationen zur Zielgruppe von ISO/IEC 15408 und zur Verwendung von ISO/IEC 15408 durch entsprechende Gruppen, die die Zielgruppe umfassen. Diese Gruppen können diesen Teil von ISO/IEC 15408 wie folgt verwenden:

- a) Verbraucher, die diesen Teil von ISO/IEC 15408 beim Auswählen von Komponenten in der Formulierung von Vertrauenswürdigkeitsanforderungen zur Erfüllung von in einem PP oder einer ST ausgedrückten Sicherheitszielsetzungen verwenden, um den erforderlichen Grad der Vertrauenswürdigkeit des TOEs zu bestimmen.
- b) Entwickler, die mit der Erstellung eines TOEs auf tatsächliche oder angenommene Sicherheitsanforderungen von Verbrauchern reagieren, verweisen auf diesen Teil von ISO/IEC 15408 bei der Interpretation von Aussagen zu Vertrauenswürdigkeitsanforderungen und der Bestimmung von Ansätzen zur Vertrauenswürdigkeit von TOEs.
- c) Evaluatoren, die die in diesem Teil von ISO/IEC 15408 definierten Vertrauenswürdigkeitsanforderungen als eine verpflichtende Aussage ihrer Evaluierungskriterien bei der Bestimmung der Vertrauenswürdigkeit der TOEs und bei der Evaluierung von PPs und STs verwenden.

## 1 Anwendungsbereich

Dieser Teil von ISO/IEC 15408 definiert die Vertrauenswürdigkeitsanforderungen von ISO/IEC 15408. Er enthält die Vertrauenswürdigkeitsstufen (EAL-Stufen) zur Definition einer Skala zum Messen der Vertrauenswürdigkeit von Komponenten-Evaluierungsgegenständen (TOEs), die zusammengesetzten Sicherheitspakete (CAPs) zur Definition einer Skala zum Messen der Vertrauenswürdigkeit von zusammengesetzten TOEs, die einzelnen Vertrauenswürdigkeitskomponenten, aus denen die Vertrauenswürdigkeitsstufen und Pakete zusammengesetzt sind, sowie die Kriterien zur Evaluierung von Schutzprofilen (PPs) und Sicherheitsvorgaben (STs).

## 2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

## 3 Begriffe, Symbole und Abkürzungen

Für die Anwendung dieses Dokuments gelten die Begriffe, Symbole und Abkürzungen nach ISO/IEC 15408-1.

## 4 Übersicht

### 4.1 Aufbau dieses Teils von ISO/IEC 15408

Abschnitt 5 beschreibt das in den Vertrauenswürdigkeitsanforderungen dieses Teils von ISO/IEC 15408 verwendete Paradigma.

Abschnitt 6 beschreibt die Struktur der Darstellung der Vertrauenswürdigkeitsklassen, -familien und -komponenten, der Vertrauenswürdigkeitsstufen und ihrer Beziehungen sowie den Aufbau der zusammengesetzten Sicherheitspakete. Er charakterisiert außerdem die in Abschnitt 9 bis Abschnitt 16 dargestellten Klassen und Familien der Vertrauenswürdigkeit.

Abschnitt 7 bietet ausführliche Definitionen der EAL-Stufen.

Abschnitt 8 bietet ausführliche Definitionen CAPs.

Abschnitt 9 bis Abschnitt 16 bieten die ausführlichen Definitionen der Vertrauenswürdigkeitsklassen nach diesem Teil von ISO/IEC 15408.

Anhang A bietet weitere Erklärungen und Beispiele der Konzepte hinter der Entwicklungsklasse.

Anhang B bietet eine Erklärung der Konzepte hinter Evaluierungen zusammengesetzter TOEs und der Klasse „Zusammensetzung“.

Anhang C bietet eine Zusammenfassung der Abhängigkeiten zwischen den Vertrauenswürdigkeitskomponenten.

Anhang D bietet eine Querverweisung zwischen PPs und den Familien und Komponenten der Klasse APE.

Anhang E bietet eine Querverweisung zwischen den EAL-Stufen und den Vertrauenswürdigkeitskomponenten.

Anhang F bietet eine Querverweisung zwischen den CAPs und den Vertrauenswürdigkeitskomponenten.

## **5 Paradigma für Vertrauenswürdigkeit**

Der Zweck dieses Abschnitts ist die Beschreibung der Philosophie, die den Ansatz zur Vertrauenswürdigkeit in ISO/IEC 15408 untermauert. Ein Verständnis dieses Abschnitts erlaubt dem Leser, den Grundgedanken hinter den Vertrauenswürdigkeitsanforderungen nach diesem Teil von ISO/IEC 15408 zu verstehen.

### **5.1 Philosophie von ISO/IEC 15408**

Die Philosophie von ISO/IEC 15408 besagt, dass Bedrohungen der Sicherheit und Verpflichtungen organisatorischer Sicherheitspolitik deutlich formuliert sein sollten und dass die vorgeschlagenen Sicherheitsmaßnahmen nachweisbar für den beabsichtigten Zweck ausreichen.

Außerdem sollten Maßnahmen getroffen werden, um die Wahrscheinlichkeit von Anfälligkeiten, die Möglichkeiten zum Verwenden (d. h. zum absichtlichen Ausnutzen oder unabsichtlichen Auslösen) einer Anfälligkeit und den Umfang des Schadens zu verringern, der durch das Verwenden einer Anfälligkeit eintreten könnte. Zusätzlich sollten Maßnahmen getroffen werden, die eine anschließende Identifizierung der Anfälligkeiten und die Beseitigung, Umgehung und/oder Benachrichtigung ermöglichen, dass die Anfälligkeit ausgenutzt oder ausgelöst wurde.

### **5.2 Ansatz für Vertrauenswürdigkeit**

Die Philosophie von ISO/IEC 15408 ist die Bereitstellung von Vertrauenswürdigkeit auf Grundlage von Evaluierung (aktiver Untersuchung) eines IT-Produkts, das als vertrauenswürdig vorgesehen ist. Evaluierung ist das traditionelle Mittel zur Bereitstellung von Vertrauenswürdigkeit und bildet die Grundlage für vorgeordnete Dokumente zu Evaluierungskriterien. ISO/IEC 15408 übernimmt durch das Abstimmen bestehender Ansätze dieselbe Philosophie. ISO/IEC 15408 rät, die Gültigkeit der Dokumentation und des entsprechenden IT-Produkts von fachkundigen Evaluatoren messen zu lassen und dabei zunehmenden Wert auf Umfang, Tiefe und Strenge zu legen.

ISO/IEC 15408 schließt die relativen Vorzüge anderer Mittel zur Schaffung von Vertrauenswürdigkeit nicht aus und kommentiert diese auch nicht. Es erfolgt weiterhin Forschung in Hinblick auf alternative Möglichkeiten zur Schaffung von Vertrauenswürdigkeit. Wenn aus diesen Forschungsaktivitäten ausgereifte alternative Ansätze erwachsen, werden diese für die Aufnahme in ISO/IEC 15408 berücksichtigt, die bereits für deren spätere Aufnahme entsprechend aufgebaut ist.

#### **5.2.1 Bedeutung von Anfälligkeiten**

Es wird angenommen, dass es Bedrohungsagenten gibt, die aktiv versuchen, Möglichkeiten zum Verletzen von Sicherheitspolitiken sowohl zur Erlangung unerlaubter Vorteile als auch für wohlgemeinte, aber dennoch unsichere Aktionen auszunutzen. Bedrohungsagenten können auch versehentlich Sicherheitsanfälligkeiten auslösen, die der Organisation Schaden zufügen. Durch das Bedürfnis zur Verarbeitung sensibler Informationen und den Mangel an Verfügbarkeit ausreichend vertrauenswürdiger Produkte entsteht ein erhebliches Risiko durch Ausfälle der IT. Daher ist es wahrscheinlich, dass IT-Sicherheitsverstöße zu erheblichen Verlusten führen können.

IT-Sicherheitsverstöße entstehen durch absichtliches Ausnutzen oder unabsichtliches Auslösen von Anfälligkeiten in IT-Anwendungen großer Unternehmen.

Es sollten Schritte zur Verhinderung von in IT-Produkten entstehenden Anfälligkeiten eingeleitet werden. Bis zu einem machbaren Umfang sollten Anfälligkeiten:

- a) beseitigt werden – das heißt, es sollten aktiv Schritte unternommen werden, um alle ausführbaren Anfälligkeiten aufzudecken, zu entfernen oder aufzuheben;
- b) minimiert werden – das heißt, es sollten aktiv Schritte unternommen werden, um die potentiellen Auswirkungen jeglicher Ausführung von Anfälligkeiten auf einen annehmbaren Restwert zu reduzieren;
- c) überwacht werden – das heißt, es sollten aktiv Schritte unternommen werden, um jegliche Versuche zum Ausführen einer verbleibenden Anfälligkeit zu erkennen, damit Schritte zur Begrenzung des Schadens eingeleitet werden können.

### 5.2.2 Ursachen von Anfälligkeiten

Anfälligkeiten können auftreten durch Fehler:

- a) in den Anforderungen – das heißt, ein IT-Produkt kann zwar alle von ihm geforderten Funktionen und Eigenschaften besitzen, aber immer noch Anfälligkeiten enthalten, die es in Hinblick auf Sicherheit ungeeignet oder unwirksam machen;
- b) in der Entwicklung – das heißt, ein IT-Produkt erfüllt nicht die Spezifikationen und/oder Anfälligkeiten wurden durch schlechte Entwicklungsrichtlinien oder fehlerhafte Designentscheidungen eingebracht;
- c) im Betrieb – das heißt, ein IT-Produkt wurde ordnungsgemäß nach einer korrekten Spezifikation erstellt, aber Anfälligkeiten wurden durch unzureichende Kontrollen im Betrieb eingebracht.

### 5.2.3 ISO/IEC 15408 Vertrauenswürdigkeit

Vertrauenswürdigkeit ist die Grundlage für Vertrauen, dass ein IT-Produkt seine Sicherheitszielsetzungen erfüllt. Vertrauenswürdigkeit kann aus Verweisungen auf Quellen wie unbegründeten Behauptungen, relevante Vorerfahrung oder gezielte Erfahrung abgeleitet werden. ISO/IEC 15408 bietet allerdings Vertrauenswürdigkeit durch aktive Untersuchung. Aktive Untersuchung ist eine Evaluierung des IT-Produkts zur Bestimmung seiner Sicherheitseigenschaften.

### 5.2.4 Vertrauenswürdigkeit durch Evaluierung

Evaluierung ist das traditionelle Mittel zur Schaffung von Vertrauenswürdigkeit und bildet die Grundlage für den Ansatz von ISO/IEC 15408. Evaluierungstechniken beinhalten, ohne darauf beschränkt zu sein:

- a) Analyse und Überprüfung von Prozess(en) und Verfahren;
- b) Überprüfung, dass Prozess(e) und Verfahren angewendet werden;
- c) Analyse der Übereinstimmung zwischen TOE-Designdarstellungen;
- d) Analyse der TOE-Designdarstellung gegen die Anforderungen;
- e) Verifizierung der Nachweise;
- f) Analyse der Leitliniendokumente;
- g) Analyse der entwickelten Funktionsprüfungen und der bereitgestellten Ergebnisse;
- h) unabhängige Funktionsprüfung;
- i) Analyse auf Anfälligkeiten (einschließlich Fehlerannahme);
- j) Penetrationstest.

### **5.3 ISO/IEC 15408 Vertrauenswürdigkeitsskala**

Die Philosophie von ISO/IEC 15408 versichert, dass höherer Evaluierungsaufwand zu höherer Vertrauenswürdigkeit führt, und dass das Ziel darin besteht, den geringstmöglichen Aufwand zu betreiben, der erforderlich ist, um die geforderte Vertrauenswürdigkeitsstufe zu erreichen. Der zunehmende Grad an Aufwand basiert auf:

- a) dem Umfang – das heißt, der Aufwand ist größer, weil ein größerer Teil des IT-Produkts eingebunden wird;
- b) der Tiefe – das heißt, der Aufwand ist größer, weil er sich auf einen feineren Designgrad und Einzelheiten der Implementierung bezieht;
- c) der Strenge – das heißt, der Aufwand ist größer, weil er in einer strukturierteren und formaleren Art und Weise eingebracht wird.

## **6 Vertrauenswürdigkeitskomponenten**

### **6.1 Aufbau der Vertrauenswürdigkeitsklassen, -familien und -komponenten**

Die folgenden Unterabschnitte beschreiben die verwendeten Konstrukte zur Darstellung von Vertrauenswürdigkeitsklassen, -familien und -komponenten.

Bild 1 zeigt die in diesem Teil von ISO/IEC 15408 definierten SARs. Es ist zu beachten, dass auf die abstrakteste Sammlung an SARs als eine Klasse verwiesen wird. Jede Klasse enthält Vertrauenswürdigkeitsfamilien, die Vertrauenswürdigkeitskomponenten enthalten, die wiederum Vertrauenswürdigkeitselemente enthalten. Klassen und Familien werden zur Bereitstellung einer Taxonomie für die Klassifizierung von SARs verwendet, während Komponenten zur Spezifizierung von SARs in einem PP/einer ST verwendet werden.

#### **6.1.1 Struktur der Vertrauenswürdigkeitsklassen**

Bild 1 stellt die Struktur der Vertrauenswürdigkeitsklassen dar.

##### **6.1.1.1 Klassenname**

Jeder Vertrauenswürdigkeitsklasse ist ein eindeutiger Name zugewiesen. Der Name deutet auf die von der Vertrauenswürdigkeitsklasse behandelten Themen hin.

Außerdem wird eine eindeutige Kurzform für den Namen der Vertrauenswürdigkeitsklasse bereitgestellt. Dies ist das vorrangige Mittel zur Verweisung auf die Vertrauenswürdigkeitsklasse. Die festgelegte Konvention ist ein „A“ gefolgt von zwei Buchstaben mit Bezug zum Klassennamen.

##### **6.1.1.2 Klasseneinleitung**

Jede Vertrauenswürdigkeitsklasse hat einen einleitenden Unterabschnitt, der die Zusammensetzung der Klasse beschreibt, und erläuternden Text zum Zweck der Klasse enthält.

##### **6.1.1.3 Vertrauenswürdigkeitsfamilien**

Jede Vertrauenswürdigkeitsklasse enthält mindestens eine Vertrauenswürdigkeitsfamilie. Die Struktur der Vertrauenswürdigkeitsfamilien ist in folgendem Unterabschnitt beschrieben.

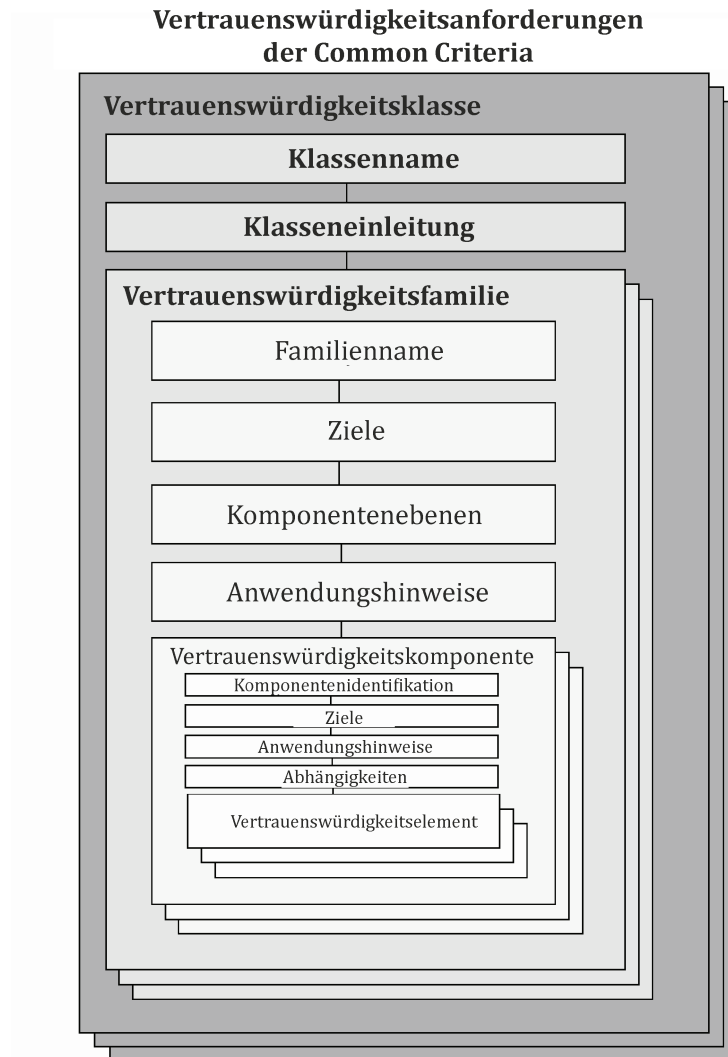


**Bild 1 — Hierarchie von Vertrauenswürdigkeitsklasse/-familie/-komponente/-element**

## 6.1.2 Struktur der Vertrauenswürdigkeitsfamilien

Bild 1 stellt die Struktur der Vertrauenswürdigkeitsfamilien dar.

### 6.1.2.1 Familiename

Jeder Vertrauenswürdigkeitsfamilie ist ein eindeutiger Name zugewiesen. Der Name enthält beschreibende Informationen zu den behandelten Themen der Vertrauenswürdigkeitsfamilie. Jede Vertrauenswürdigkeitsfamilie ist in eine Vertrauenswürdigkeitsklasse eingeordnet, die weitere Familien mit gleichem Zweck enthält.

Außerdem wird eine eindeutige Kurzform für den Namen der Vertrauenswürdigkeitsfamilie bereitgestellt. Diese ist das vorrangige Mittel zur Verweisung auf die Vertrauenswürdigkeitsfamilie. Die festgelegte Konvention ist, dass die Kurzform des Klassennamens verwendet wird, gefolgt von einem Unterstrich und anschließend drei Buchstaben mit Bezug zum Familiennamen.

#### 6.1.2.2 Ziele

Der Unterabschnitt „Ziele“ der Vertrauenswürdigkeitsfamilie stellt den Zweck der Vertrauenswürdigkeitsfamilie dar.

Dieser Unterabschnitt beschreibt die Ziele, insbesondere die Ziele in Bezug auf das Vertrauenswürdigkeitsparadigma von ISO/IEC 15408, das von der Familie behandelt wird. Die Beschreibung der Vertrauenswürdigkeitsfamilie ist allgemein gehalten. Alle erforderlichen Einzelheiten für die Ziele sind in der jeweiligen Vertrauenswürdigkeitskomponente enthalten.

#### 6.1.2.3 Komponentenebenen

Jede Vertrauenswürdigkeitsfamilie enthält eine oder mehrere Vertrauenswürdigkeitskomponenten. Dieser Unterabschnitt der Vertrauenswürdigkeitsfamilie beschreibt die verfügbaren Komponenten und erklärt zwischen ihnen bestehende Unterschiede. Der wesentliche Zweck des Unterabschnitts ist die Differenzierung zwischen den Vertrauenswürdigkeitskomponenten, nachdem festgestellt wurde, dass die Vertrauenswürdigkeitsfamilie ein erforderlicher oder sinnvoller Teil der SARs für ein PP/eine ST ist.

Vertrauenswürdigkeitsfamilien mit mehr als einer Komponente werden eingestuft und für die Art der Einstufung wird eine Begründung bereitgestellt. Diese Begründung bezieht sich auf den Umfang, die Tiefe und/oder die Strenge.

#### 6.1.2.4 Anwendungshinweise

Falls vorhanden, enthält der Unterabschnitt „Anwendungshinweise“ der Vertrauenswürdigkeitsfamilie zusätzliche Informationen zur Vertrauenswürdigkeitsfamilie. Diese Informationen sollten von besonderem Interesse für Anwender der Vertrauenswürdigkeitsfamilie (z. B. PP-/ST-Autoren, Designer von TOEs, Evaluatoren) sein. Die Darstellung ist informativ und enthält beispielsweise Warnungen zu Anwendungsgrenzen und Bereiche, für die besondere Beachtung erforderlich sein kann.

#### 6.1.2.5 Vertrauenswürdigkeitskomponenten

Jede Vertrauenswürdigkeitsfamilie enthält mindestens eine Vertrauenswürdigkeitskomponente. Die Struktur der Vertrauenswürdigkeitskomponenten ist in folgendem Unterabschnitt beschrieben.

### 6.1.3 Struktur der Vertrauenswürdigkeitskomponenten

Bild 2 stellt die Struktur der Vertrauenswürdigkeitskomponenten dar.

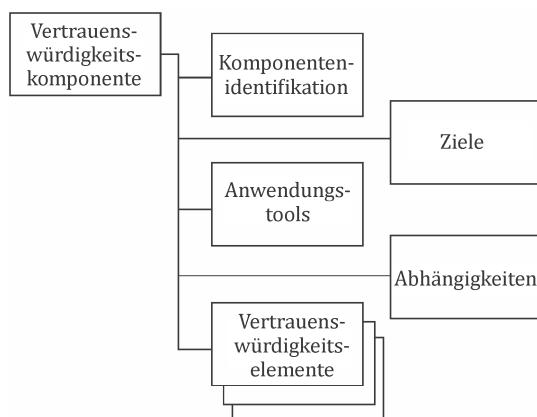


**Bild 2 — Struktur der Vertrauenswürdigkeitskomponenten**

Die Beziehung zwischen den Komponenten einer Familie wird als Konvention über eine Fettmarkierung hervorgehoben. Teile der Anforderungen, die neu oder erweitert sind oder die über die Anforderungen der vorherigen Komponente innerhalb einer Hierarchie hinaus geändert wurden, sind fett hervorgehoben.

#### **6.1.3.1 Komponentenidentifikation**

Der Unterabschnitt „Komponentenidentifikation“ bietet beschreibende Informationen, die zur Identifizierung, Kategorisierung, Registrierung und Verweisung einer Komponente erforderlich sind.

Jeder Vertrauenswürdigkeitskomponente ist ein eindeutiger Name zugewiesen. Der Name enthält beschreibende Informationen zu den behandelten Themen der Vertrauenswürdigkeitskomponente. Jede Vertrauenswürdigkeitskomponente ist in eine Vertrauenswürdigkeitsfamilie eingeordnet, die ihre Sicherheitszielsetzung teilt.

Außerdem wird eine eindeutige Kurzform für den Namen der Vertrauenswürdigkeitskomponente bereitgestellt. Diese ist das vorrangige Mittel zur Verweisung auf die Vertrauenswürdigkeitskomponente. Die festgelegte Konvention ist, dass die Kurzform des Familiennamens verwendet wird, gefolgt von einem Punkt und einem numerischen Zeichen. Die numerischen Zeichen für Komponenten innerhalb einer Familie werden fortlaufend zugewiesen, beginnend bei 1.

#### **6.1.3.2 Ziele**

Falls vorhanden, enthält der Unterabschnitt „Ziele“ der Vertrauenswürdigkeitskomponente bestimmte Ziele für die jeweilige Vertrauenswürdigkeitskomponente. Bei Vertrauenswürdigkeitskomponenten, die diesen Unterabschnitt aufweisen, werden hier der besondere Zweck der Komponente und eine ausführlichere Erklärung der Ziele dargestellt.

#### **6.1.3.3 Anwendungshinweise**

Falls vorhanden, enthält der Unterabschnitt „Anwendungshinweise“ der Vertrauenswürdigkeitskomponente zusätzliche Informationen, um die Verwendung der Komponente zu erleichtern.

#### **6.1.3.4 Abhängigkeiten**

Wenn eine Komponente für sich genommen nicht ausreichend und auf das Vorhandensein einer anderen Komponente angewiesen ist, entstehen Abhängigkeiten unter Vertrauenswürdigkeitskomponenten.

Jede Vertrauenswürdigkeitskomponente bietet eine vollständige Liste an Abhängigkeiten zu anderen Vertrauenswürdigkeitskomponenten. Manche Komponenten können auch „keine Abhängigkeiten“ auflisten, um anzuzeigen, dass keine Abhängigkeiten identifiziert wurden. Die abhängigen Komponenten können Abhängigkeiten zu weiteren Komponenten haben.

Die Abhängigkeitsliste identifiziert die minimale Reihe an Vertrauenswürdigkeitskomponenten, auf die sich verlassen wird. Komponenten, die zu einer Komponente in der Abhängigkeitsliste hierarchisch sind, dürfen auch zur Erfüllung der Abhängigkeit verwendet werden.

In bestimmten Situationen kann es vorkommen, dass die angegebenen Abhängigkeiten nicht anwendbar sein könnten. Durch die Angabe einer Begründung, warum eine bestimmte Abhängigkeit nicht anwendbar ist, darf der PP-/ST-Autor auch auswählen, dass die Abhängigkeit nicht erfüllt wird.

#### **6.1.3.5 Vertrauenswürdigkeitselemente**

Für jede Vertrauenswürdigkeitskomponente wird eine Reihe an Vertrauenswürdigkeitselementen bereitgestellt. Ein Vertrauenswürdigkeitselement ist eine Sicherheitsanforderung, die bei weiterer Aufteilung zu keinem sinnvollen Evaluierungsergebnis führen würde. Es ist die kleinste Einheit der in von ISO/IEC 15408 angegebenen Sicherheitsanforderungen.

Jedes Vertrauenswürdigkeitselement wird als zu einer der drei Sätze an Vertrauenswürdigkeitselementen zugehörig identifiziert.

- a) Elemente der Entwickleraktionen: die Aktivitäten, die vom Entwickler ausgeführt werden müssen. Dieser Satz an Aktionen wird über das in den folgenden Elementsätzen verwiesene Nachweismaterial weiter qualifiziert. Anforderungen für Entwickleraktionen werden über Anhängen des Buchstabens „D“ (en: developer) an die Elementnummer identifiziert.
- b) Elemente von Inhalt und Darstellung des Nachweises: der erforderliche Nachweis, was der Nachweis darlegen muss und welche Informationen der Nachweis vermitteln muss. Anforderungen für Inhalt und Darstellung des Nachweises werden über Anhängen des Buchstabens „C“ (en: content) an die Elementnummer identifiziert.
- c) Elemente der Evaluatoraktionen: die Aktivitäten, die vom Evaluator ausgeführt werden müssen. Dieser Satz an Aktionen enthält explizit die Bestätigung, dass die vorgeschriebenen Anforderungen in den Elementen zu Inhalt und Darstellung des Nachweises erfüllt wurden. Er enthält außerdem explizite Aktionen und Analyse, die zusätzlich zu den bereits vom Entwickler ausgeführten Aktionen durchgeführt werden müssen. Implizite Evaluatoraktionen müssen ebenfalls als Ergebnis von Elementen zu Entwickleraktionen durchgeführt werden, die nicht von Elementen zu Inhalt und Darstellung des Nachweises abgedeckt sind. Anforderungen für Evaluatoraktionen werden über Anhängen des Buchstabens „E“ (en: evaluator) an die Elementnummer identifiziert.

Die Entwickleraktionen und Inhalt und Darstellung des Nachweises definieren die Vertrauenswürdigkeitsanforderungen, die zur Abbildung der Verantwortung des Entwicklers zum Nachweis der Vertrauenswürdigkeit des TOEs zur Erfüllung der SFRs eines PP oder einer ST verwendet wird.

Die Evaluatoraktionen definieren die Verantwortung des Evaluators bei den zwei Aspekten der Evaluierung. Der erste Aspekt ist die Validierung des PP/der ST in Übereinstimmung mit den Klassen APE und ASE in den Abschnitten „APE: Protection Profile evaluation“ und „ASE: Security Target evaluation“. Der zweite Aspekt ist die Verifizierung der Konformität des TOEs mit seinen SFRs und SARs. Durch den Nachweis, dass das PP/die ST gültig ist und dass die Anforderungen vom TOE erfüllt werden, kann der Evaluator eine Grundlage für das Vertrauen schaffen, dass der TOE das definierte Sicherheitsproblem in seiner Betriebsumgebung löst.

Die Elemente der Entwickleraktionen, Elemente von Inhalt und Darstellung des Nachweises und die expliziten Elemente der Evaluatoraktionen identifizieren den Aufwand des Evaluators, der zum Verifizieren der in der ST des TOEs gemachten Sicherheitsansprüche aufgebracht werden muss.

#### 6.1.4 Vertrauenswürdigkeitselemente

Jedes Element stellt eine zu erfüllende Anforderung dar. Diese Aussagen zu Anforderungen sind auf Klarheit, Knappheit und Eindeutigkeit ausgelegt. Daher gibt es keine zusammengesetzten Sätze: jede trennbare Anforderung ist als einzelnes Element angegeben.

#### 6.1.5 Komponententaxonomie

Dieser Teil von ISO/IEC 15408 enthält Klassen von Familien und Komponenten, die auf Grundlage zusammengehöriger Vertrauenswürdigkeit gruppiert sind. Zu Beginn jeder Klasse gibt es ein Diagramm, das die Familien in der Klasse und die Komponenten in jeder Familie anzeigt.



**Bild 3 — Muster eines Klassenaufbaudiagramms**

Bild 3 oben zeigt eine Klasse, die eine einzige Familie enthält. Die Familie enthält drei Komponenten, die linear hierarchisch sind (d. h. Komponente 2 erfordert mehr als Komponente 1 bezüglich bestimmter Aktionen, bestimmter Nachweise oder Strenge der Aktionen oder der Nachweise). Die Vertrauenswürdigkeitsfamilien

in diesem Teil von ISO/IEC 15408 sind alle linear hierarchisch, wobei Linearität kein verpflichtendes Kriterium für Vertrauenswürdigkeitsfamilien ist, die möglicherweise zukünftig hinzugefügt werden.

## 6.2 Struktur der EAL-Stufen

Bild 4 zeigt die in diesem Teil von ISO/IEC 15408 definierten EAL-Stufen und die mit ihnen verbundenen Strukturen. Es ist zu beachten, dass das Bild zwar den Inhalt der Vertrauenswürdigkeitskomponenten zeigt, es aber vorgesehen ist, diese Informationen über Verweisung auf die eigentlichen in von ISO/IEC 15408 definierten Komponenten in einer EAL-Stufe aufzunehmen.

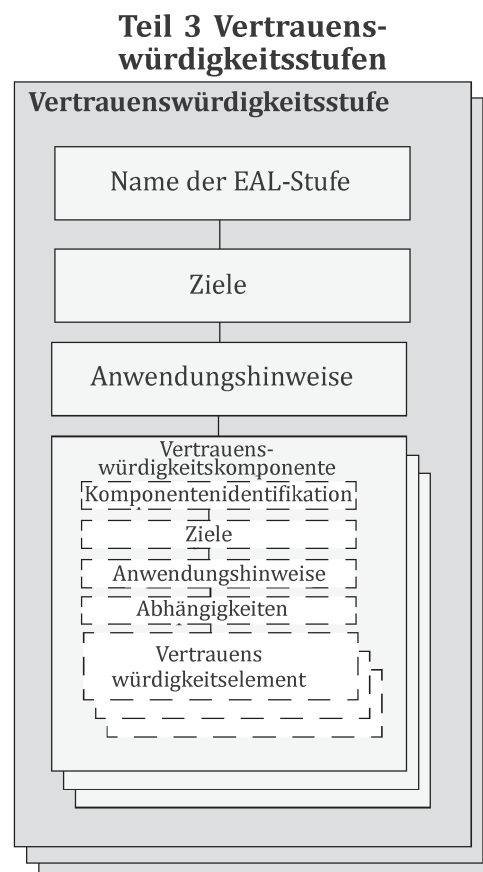


**Bild 4 — Struktur der EAL-Stufen**

### 6.2.1 Name der EAL-Stufe

Jeder EAL-Stufe ist ein eindeutiger Name zugewiesen. Der Name enthält beschreibende Informationen zum Zweck der EAL-Stufe.

Außerdem wird eine eindeutige Kurzform für den Namen der EAL-Stufe bereitgestellt. Diese ist das vorrangige Mittel zur Verweisung auf die EAL-Stufe.

### 6.2.2 Ziele

Der Unterabschnitt „Ziele“ der EAL-Stufe stellt den Zweck der EAL-Stufe dar.

### 6.2.3 Anwendungshinweise

Falls vorhanden, enthält der Unterabschnitt „Anwendungshinweise“ der EAL-Stufe Informationen von besonderem Interesse für Anwender der EAL-Stufe (z. B. PP-/ST-Autoren, Designer von auf diese EAL-Stufe

abzielenden TOEs, Evaluatoren). Die Darstellung ist informativ und enthält beispielsweise Warnungen zu Anwendungsgrenzen und Bereiche, für die besondere Beachtung erforderlich sein kann.

#### 6.2.4 Vertrauenswürdigkeitskomponenten

Für jede EAL-Stufe wird eine Reihe an Vertrauenswürdigkeitskomponenten bereitgestellt.

Ein höherer Grad an Vertrauenswürdigkeit als von einer bestimmten EAL-Stufe bereitgestellt kann erreicht werden durch

- Einbindung zusätzlicher Vertrauenswürdigkeitskomponenten aus anderen Vertrauenswürdigkeitsfamilien oder
- Austausch einer Vertrauenswürdigkeitskomponente durch eine Vertrauenswürdigkeitskomponente einer höheren Stufe aus derselben Vertrauenswürdigkeitsfamilie.

#### 6.2.5 Beziehung zwischen Vertrauenswürdigkeit und Vertrauenswürdigkeitsstufe

Bild 5 zeigt die in von ISO/IEC 15408 definierte Beziehung zwischen den SARs und den Vertrauenswürdigkeitsstufen. Während Vertrauenswürdigkeitskomponenten weiter zerlegt werden in Vertrauenswürdigkeitselemente, können Vertrauenswürdigkeitsstufen können nicht einzeln auf diese Vertrauenswürdigkeitselemente verweisen. Es ist zu beachten, dass der Pfeil im Bild eine Verweisung von einer EAL-Stufe auf eine Vertrauenswürdigkeitskomponente innerhalb der Klasse darstellt, in der sie definiert ist.

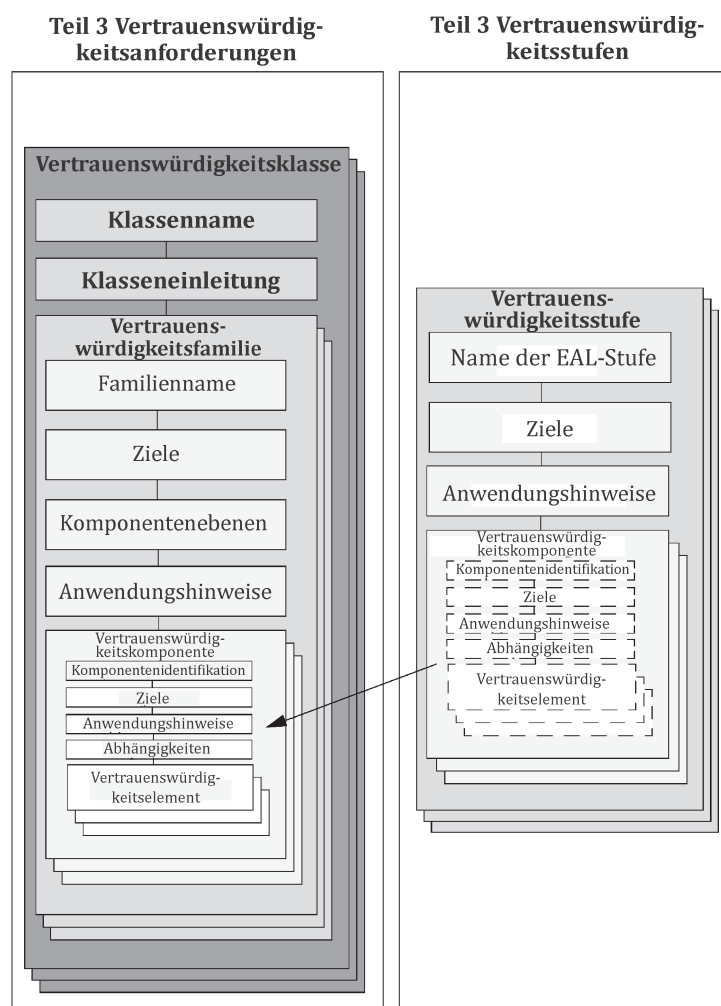


Bild 5 — Verknüpfung von Vertrauenswürdigkeit und Vertrauenswürdigkeitsstufe

### 6.3 Struktur der CAPs

Die Struktur der CAPs ähnelt der Struktur der EAL-Stufen. Der wesentliche Unterschied zwischen diesen beiden Paketarten ist der TOE-Typ, für den sie gelten; die EAL-Stufen gelten für Komponenten-TOEs und die CAPs gelten für zusammengesetzte TOEs.

Bild 6 zeigt die in diesem Teil von ISO/IEC 15408 definierten CAPs und die mit ihnen verbundenen Strukturen. Es ist zu beachten, dass das Bild zwar den Inhalt der Vertrauenswürdigkeitskomponenten zeigt, es aber vorgesehen ist, diese Informationen über Verweisung auf die eigentlichen in von ISO/IEC 15408 definierten Komponenten in einer CAP aufzunehmen.

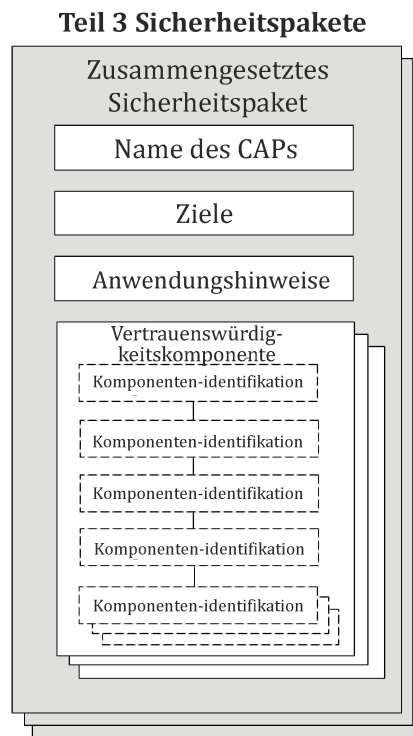


**Bild 6 — Struktur der CAPs**

#### 6.3.1 Name des CAPs

Jedem CAP ist ein eindeutiger Name zugewiesen. Der Name enthält beschreibende Informationen zum Zweck des CAPs.

Außerdem wird eine eindeutige Kurzform für den Namen des CAPs bereitgestellt. Diese ist das vorrangige Mittel zur Verweisung auf das CAP.

#### 6.3.2 Ziele

Der Unterabschnitt „Ziele“ des CAPs stellt den Zweck des CAPs dar.

#### 6.3.3 Anwendungshinweise

Falls vorhanden, enthält der Unterabschnitt „Anwendungshinweise“ des CAPs Informationen von besonderem Interesse für Anwender des CAPs (z. B. PP-/ST-Autoren, Integratoren von auf dieses CAP abzielenden zusammengesetzten TOEs, Evaluatoren). Die Darstellung ist informativ und enthält beispielsweise Warnungen zu Anwendungsgrenzen und Bereiche, für die besondere Beachtung erforderlich sein kann.

#### **6.3.4 Vertrauenswürdigkeitskomponenten**

Für jedes CAP wird eine Reihe von Vertrauenswürdigkeitskomponenten bereitgestellt.

Einige Abhängigkeiten identifizieren die während der Evaluierung der abhängigen Komponente durchgeführten Aktivitäten, auf die sich die Aktivität des zusammengesetzten TOE verlässt. Wenn nicht explizit identifiziert ist, dass die Abhängigkeit zu einer abhängigen Komponentenaktivität besteht, besteht die Abhängigkeit zu einer anderen Evaluierungsaktivität des zusammengesetzten TOEs.

Ein höherer Grad an Vertrauenswürdigkeit als von einem bestimmten CAP bereitgestellt kann erreicht werden durch

- a) Einbindung zusätzlicher Vertrauenswürdigkeitskomponenten aus anderen Vertrauenswürdigkeitsfamilien oder
- b) Austausch einer Vertrauenswürdigkeitskomponente durch eine Vertrauenswürdigkeitskomponente einer höheren Stufe aus derselben Vertrauenswürdigkeitsfamilie.

Die Komponenten „ACO: Zusammensetzung“, die in den CAPs enthalten sind, sollten nicht als Erweiterungen für Evaluierungen von Komponenten-TOE verwendet werden, da dies keine sinnvolle Vertrauenswürdigkeit für die Komponente bieten würde.

#### **6.3.5 Beziehung zwischen Vertrauenswürdigkeit und Vertrauenswürdigkeitsstufe**

Bild 7 zeigt die in von ISO/IEC 15408 definierte Beziehung zwischen den SARs und den zusammengesetzten Sicherheitspaketen. Während Vertrauenswürdigkeitskomponenten weiter zerlegt werden in Vertrauenswürdigkeitselemente, können Sicherheitspakete nicht einzeln auf diese Vertrauenswürdigkeitselemente verweisen. Es ist zu beachten, dass der Pfeil im Bild eine Verweisung von einem CAP auf eine Vertrauenswürdigkeitskomponente innerhalb der Klasse darstellt, in der sie definiert ist.

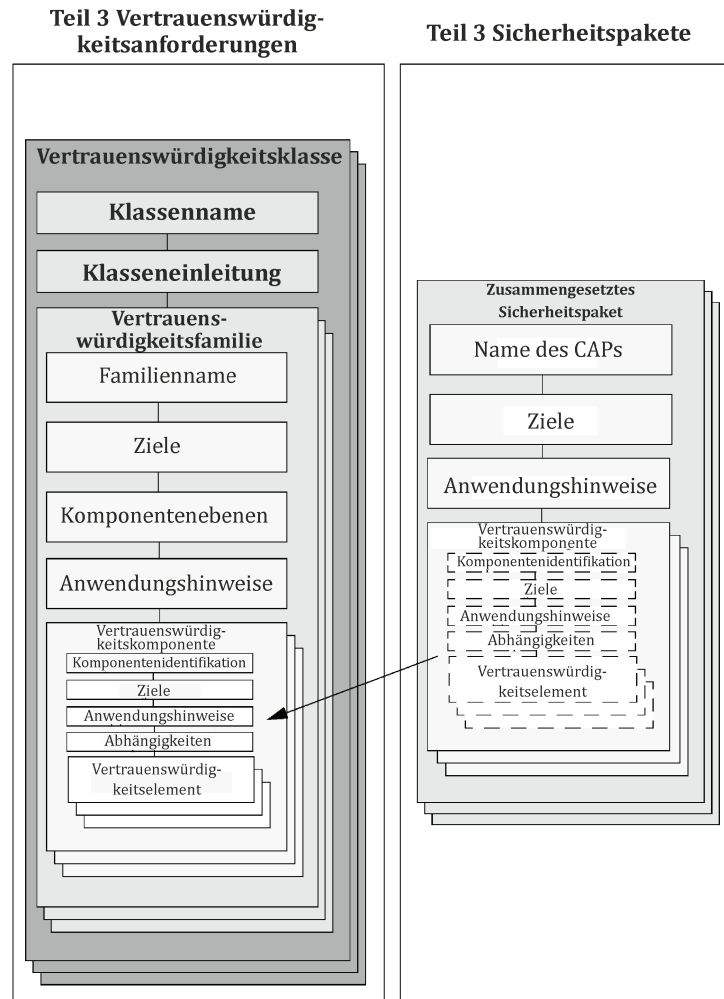


Bild 7 — Verknüpfung von Vertrauenswürdigkeit und zusammengesetztem Sicherheitspaket

## 7 Vertrauenswürdigkeitsstufen

Die Vertrauenswürdigkeitsstufen (EAL-Stufen) stellen eine ansteigende Skala dar, bei der der Grad der erreichbaren Vertrauenswürdigkeit mit den damit verbundenen Kosten und der Durchführbarkeit abgewogen wird. Der Ansatz von ISO/IEC 15408 identifiziert die einzelnen Konzepte der Vertrauenswürdigkeit in einem TOE am Ende der Evaluierung sowie der Aufrechterhaltung dieser Vertrauenswürdigkeit über den Betriebszeitraum des TOEs.

Es ist wichtig darauf hinzuweisen, dass nicht alle Familien und Komponenten aus diesem Teil von ISO/IEC 15408 in den EAL-Stufen enthalten sind. Das heißt nicht, dass diese Familien und Komponenten keine sinnvolle und erstrebenswerte Vertrauenswürdigkeit bieten. Vielmehr wird erwartet, dass diese Familien und Komponenten für die Erweiterung einer EAL-Stufe in PPs und STs berücksichtigt werden, für die sie einen Nutzen bieten.

### 7.1 Übersicht über die Vertrauenswürdigkeitsstufen (EAL-Stufen)

Tabelle 1 zeigt eine Zusammenfassung der EAL-Stufen. Die Spalten stellen eine hierarchisch geordnete Reihe von EAL-Stufen dar, und die Zeilen zeigen die Vertrauenswürdigkeitsfamilien. Jede Ziffer in der sich ergebenden Matrix bezeichnet gegebenenfalls eine bestimmte Vertrauenswürdigkeitskomponente.

Wie im folgenden Unterabschnitt dargelegt, sind zur Bewertung der Vertrauenswürdigkeit eines TOEs sieben hierarchisch geordnete Vertrauenswürdigkeitsstufen in ISO/IEC 15408 definiert. Sie sind insofern

hierarchisch geordnet, dass jede EAL-Stufe eine größere Vertrauenswürdigkeit darstellt als alle niedrigeren EAL-Stufen. Die Zunahme der Vertrauenswürdigkeit von EAL-Stufe zu EAL-Stufe wird durch den Austausch einer hierarchisch höheren Vertrauenswürdigkeitskomponente derselben Vertrauenswürdigkeitsfamilie (d.h. zunehmende Strenge, Umfang und/oder Tiefe) und durch das Hinzufügen von Vertrauenswürdigkeitskomponenten aus anderen Vertrauenswürdigkeitsfamilien (d.h. Hinzufügen neuer Anforderungen) erreicht.

Diese EAL-Stufen bestehen aus einer geeigneten Kombination aus Vertrauenswürdigkeitskomponenten, die in Abschnitt 6 dieses Teils von ISO/IEC 15408 beschrieben sind. Genauer ausgedrückt enthält jede EAL-Stufe nicht mehr als eine Komponente jeder Vertrauenswürdigkeitsfamilie und alle Abhängigkeiten der Vertrauenswürdigkeit jeder Komponente werden angesprochen.

Während die EAL-Stufen in von ISO/IEC 15408 definiert sind, ist es auch möglich, weitere Kombinationen an Vertrauenswürdigkeit darzustellen. Insbesondere erlaubt der Ausdruck „Erweiterung“ das Hinzufügen von Vertrauenswürdigkeitskomponenten (aus Vertrauenswürdigkeitsfamilien, die nicht bereits in der EAL-Stufe enthalten sind) oder den Austausch von Vertrauenswürdigkeitskomponenten (durch andere, hierarchisch höhere Vertrauenswürdigkeitskomponenten derselben Vertrauenswürdigkeitsfamilie) in einer EAL-Stufe. Von allen in von ISO/IEC 15408 definierten Konstrukten zur Vertrauenswürdigkeit dürfen nur für EAL-Stufen erweitert werden. Der Ausdruck „EAL abzüglich einer einzelnen Vertrauenswürdigkeitskomponente“ wird von der Norm nicht als gültige Aussage anerkannt. Eine Erweiterung bringt die Verpflichtung für den Aussagenden mit sich, Nutzen und Mehrwert der zur EAL-Stufe hinzugefügten Vertrauenswürdigkeitskomponente zu begründen. Eine EAL-Stufe darf auch mit erweiterten Vertrauenswürdigkeitsanforderungen erweitert werden.

**Tabelle 1 — Zusammenfassung der Vertrauenswürdigkeitsstufen**

| Vertrauenswürdigkeits-<br>klasse      | Vertrauenswürdigkeits-<br>familie | Vertrauenswürdigkeitskomponenten nach<br>Vertrauenswürdigkeitsstufe |      |      |      |      |      |      |
|---------------------------------------|-----------------------------------|---------------------------------------------------------------------|------|------|------|------|------|------|
|                                       |                                   | EAL1                                                                | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| Entwicklung                           | ADV_ARC                           |                                                                     | 1    | 1    | 1    | 1    | 1    | 1    |
|                                       | ADV_FSP                           | 1                                                                   | 2    | 3    | 4    | 5    | 5    | 6    |
|                                       | ADV_IMP                           |                                                                     |      |      | 1    | 1    | 2    | 2    |
|                                       | ADV_INT                           |                                                                     |      |      |      | 2    | 3    | 3    |
|                                       | ADV_SPM                           |                                                                     |      |      |      |      | 1    | 1    |
|                                       | ADV_TDS                           |                                                                     | 1    | 2    | 3    | 4    | 5    | 6    |
| Leitliniendokumente                   | AGD_OPE                           | 1                                                                   | 1    | 1    | 1    | 1    | 1    | 1    |
|                                       | AGD_PRE                           | 1                                                                   | 1    | 1    | 1    | 1    | 1    | 1    |
| Lebenszyklus-<br>unterstützung        | ALC_CMC                           | 1                                                                   | 2    | 3    | 4    | 4    | 5    | 5    |
|                                       | ALC_CMS                           | 1                                                                   | 2    | 3    | 4    | 5    | 5    | 5    |
|                                       | ALC_DEL                           |                                                                     | 1    | 1    | 1    | 1    | 1    | 1    |
|                                       | ALC_DVS                           |                                                                     |      | 1    | 1    | 1    | 2    | 2    |
|                                       | ALC_FLR                           |                                                                     |      |      |      |      |      |      |
|                                       | ALC_LCD                           |                                                                     |      | 1    | 1    | 1    | 1    | 2    |
|                                       | ALC_TAT                           |                                                                     |      |      | 1    | 2    | 3    | 3    |
| Evaluierung der<br>Sicherheitsvorgabe | ASE_CCL                           | 1                                                                   | 1    | 1    | 1    | 1    | 1    | 1    |
|                                       | ASE_ECD                           | 1                                                                   | 1    | 1    | 1    | 1    | 1    | 1    |
|                                       | ASE_INT                           | 1                                                                   | 1    | 1    | 1    | 1    | 1    | 1    |
|                                       | ASE_OBJ                           | 1                                                                   | 2    | 2    | 2    | 2    | 2    | 2    |
|                                       | ASE_REQ                           | 1                                                                   | 2    | 2    | 2    | 2    | 2    | 2    |
|                                       | ASE_SPD                           |                                                                     | 1    | 1    | 1    | 1    | 1    | 1    |
|                                       | ASE_TSS                           | 1                                                                   | 1    | 1    | 1    | 1    | 1    | 1    |

| Vertrauenswürdigkeits-<br>klasse | Vertrauenswürdigkeits-<br>familie | Vertrauenswürdigkeitskomponenten nach<br>Vertrauenswürdigkeitsstufe |      |      |      |      |      |      |
|----------------------------------|-----------------------------------|---------------------------------------------------------------------|------|------|------|------|------|------|
|                                  |                                   | EAL1                                                                | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| Prüfungen                        | ATE_COV                           |                                                                     | 1    | 2    | 2    | 2    | 3    | 3    |
|                                  | ATE_DPT                           |                                                                     |      | 1    | 1    | 3    | 3    | 4    |
|                                  | ATE_FUN                           |                                                                     | 1    | 1    | 1    | 1    | 2    | 2    |
|                                  | ATE_IND                           | 1                                                                   | 2    | 2    | 2    | 2    | 2    | 3    |
| Anfälligkeitsbewertung           | AVA_VAN                           | 1                                                                   | 2    | 2    | 3    | 4    | 5    | 5    |

## 7.2 Einzelheiten der Vertrauenswürdigkeitsstufen

Die folgenden Unterabschnitte enthalten Definitionen zu den EAL-Stufen und heben Unterschiede zwischen den einzelnen Anforderungen und den Merkmalen dieser Anforderungen über Fettmarkierung hervor.

## 7.3 Vertrauenswürdigkeitsstufe 1 (EAL1) – funktional geprüft

### 7.3.1 Ziele

EAL1 ist anwendbar, wenn ein gewisses Vertrauen in den ordnungsgemäßen Betrieb erforderlich ist, aber die Sicherheitsbedrohungen nicht als ernst angesehen werden. Diese Stufe ist nützlich, wenn unabhängige Vertrauenswürdigkeit zur Unterstützung der Behauptung erforderlich ist, dass ausreichende Sorgfalt in Hinblick auf den Schutz persönlicher oder ähnlicher Informationen aufgebracht wurde.

EAL1 erfordert nur eine beschränkte Sicherheitsvorgabe. Es genügt, die vom TOE zu erfüllenden SFRs einfach anzugeben, anstatt sie aus Bedrohungen, OSPs und Annahmen durch Sicherheitszielsetzungen abzuleiten.

EAL1 bietet eine für den Verbraucher verfügbare Evaluierung des TOEs, einschließlich unabhängiger Prüfungen gegen eine Spezifikation sowie eine Prüfung der bereitgestellten Leitliniendokumentation. Es ist vorgesehen, dass eine Evaluierung nach EAL1 erfolgreich ohne die Hilfe des Entwicklers des TOEs und mit minimalem Aufwand durchgeführt werden könnte.

Eine Evaluierung auf dieser Stufe sollte den Nachweis liefern, dass der TOE in einer seiner Dokumentation entsprechenden Art und Weise funktioniert.

### 7.3.2 Vertrauenswürdigkeitskomponenten

**EAL1 bietet einen grundlegenden Grad an Vertrauenswürdigkeit durch eine eingeschränkte Sicherheitsvorgabe und durch eine Analyse der SFRs in dieser ST unter Verwendung einer Funktions- und Schnittstellenspezifikation sowie einer Leitliniendokumentation, um das Sicherheitsverhalten zu verstehen.**

Die Analyse wird durch eine Suche nach potentiellen Anfälligkeiten im öffentlichen Bereich („public domain“) und durch unabhängige Prüfung (Funktionsprüfung und Penetrationstest) der TSF unterstützt.

**EAL1 bietet außerdem Vertrauenswürdigkeit durch eindeutige Identifikation des TOEs und der relevanten Evaluierungsdokumente.**

**Diese EAL-Stufe bietet eine sinnvolle Zunahme der Vertrauenswürdigkeit im Vergleich zu einer nicht evaluierten IT.**

Tabelle 2 — EAL1

| Vertrauenswürdigkeitsklasse             | Vertrauenswürdigkeitskomponenten                            |
|-----------------------------------------|-------------------------------------------------------------|
| ADV: Entwicklung                        | ADV_FSP.1 Grundlegende Funktionsanforderung                 |
| AGD: Leitliniendokumente                | AGD_OPE.1 Operative Leitlinien für Benutzer                 |
|                                         | AGD_PRE.1 Vorbereitende Verfahren                           |
| ALC: Unterstützung des Lebenszyklus     | ALC_CMC.1 Kennzeichnung des TOEs                            |
|                                         | ALC_CMS.1 CM-Abdeckung des TOEs                             |
| ASE: Evaluierung der Sicherheitsvorgabe | ASE_CCL.1 Konformitätsansprüche                             |
|                                         | ASE_ECD.1 Erweiterte Komponentendefinition                  |
|                                         | ASE_INT.1 ST Einleitung                                     |
|                                         | ASE_OBJ.1 Sicherheitszielsetzungen für die Betriebsumgebung |
|                                         | ASE_REQ.1 Festgelegte Sicherheitsanforderungen              |
|                                         | ASE_TSS.1 Zusammenfassende Spezifikation des TOEs           |
| ATE: Tests                              | ATE_IND.1 Unabhängige Prüfungen – Konformität               |
| AVA: Anfälligkeitsbewertung             | AVA_VAN.1 Anfälligkeitsuntersuchung                         |

## 7.4 Vertrauenswürdigkeitsstufe 2 (EAL2) – strukturell geprüft

### 7.4.1 Ziele

EAL2 erfordert die Mitarbeit des Entwicklers bei der Bereitstellung der Designinformationen und Prüfergebnisse, sollte aber nicht mehr Aufwand für den Entwickler abverlangen, als guter Geschäftspraxis entspricht. Von daher sollte dies kein wesentlich erhöhtes Maß an Kosten oder Zeit erfordern.

EAL2 ist damit anwendbar für Situationen, in denen Entwickler oder Benutzer einen geringen oder moderaten Grad an unabhängig zugesicherter Sicherheit ohne unmittelbare Verfügbarkeit der vollständigen Entwicklungshistorie erfordern. Solche Situationen können bei der Absicherung von Altsystemen auftreten oder wenn der Zugriff für den Entwickler eingeschränkt sein kann.

### 7.4.2 Vertrauenswürdigkeitskomponenten

**EAL2** bietet Vertrauenswürdigkeit durch eine **vollständige** Sicherheitsvorgabe und durch eine Analyse der SFRs in dieser ST unter Verwendung einer Funktions- und Schnittstellenspezifikation, einer Leitliniendokumentation **und einer grundlegenden Beschreibung der Architektur des TOEs**, um das Sicherheitsverhalten zu verstehen.

Die Analyse wird unterstützt durch unabhängige Prüfung der TSF, **durch Nachweis der Entwicklerprüfung auf Grundlage der Funktionsspezifikation, durch ausgewählte unabhängige Bestätigung der Prüfergebnisse des Entwicklers sowie durch eine Anfälligkeitsanalyse (auf Grundlage von Funktionsspezifikation, TOE-Design, Beschreibung der Sicherheitsarchitektur und bereitgestelltem Nachweis der Leitlinien), die die Widerstandsfähigkeit gegen eindringende Angreifer mit grundlegendem Angriffspotential nachweist.**

**EAL2** bietet außerdem Vertrauenswürdigkeit durch **Verwendung** eines **Konfigurationsmanagementsystems** und durch **Nachweis** von **sicheren Lieferverfahren**.

Diese EAL-Stufe **ist** eine sinnvolle Zunahme der Vertrauenswürdigkeit **im Vergleich zu EAL1 durch die Forderung nach Entwicklerprüfungen, nach einer Anfälligkeitsanalyse (zusätzlich zur Suche im öffentlichen Bereich) und nach unabhängiger Prüfung auf Grundlage ausführlicherer TOE-Spezifikationen.**

**Tabelle 3 — EAL2**

| Vertrauenswürdigkeitsklasse             | Vertrauenswürdigkeitskomponenten                          |
|-----------------------------------------|-----------------------------------------------------------|
| ADV: Entwicklung                        | ADV_ARC.1 Beschreibung der Sicherheitsarchitektur         |
|                                         | ADV_FSP.2 Sicherheit durchsetzende Funktionsspezifikation |
|                                         | ADV_TDS.1 Grundsätzliches Design                          |
| AGD: Leitliniendokumente                | AGD_OPE.1 Operative Leitlinien für Benutzer               |
|                                         | AGD_PRE.1 Vorbereitende Verfahren                         |
| ALC: Unterstützung des Lebenszyklus     | ALC_CMC.2 Verwendung eines CM-Systems                     |
|                                         | ALC_CMS.2 CM Abdeckung für Teile des TOEs                 |
|                                         | ALC_DEL.1 Lieferverfahren                                 |
| ASE: Evaluierung der Sicherheitsvorgabe | ASE_CCL.1 Konformitätsansprüche                           |
|                                         | ASE_ECD.1 Erweiterte Komponentendefinition                |
|                                         | ASE_INT.1 ST Einleitung                                   |
|                                         | ASE_OBJ.2 Sicherheitszielsetzungen                        |
|                                         | ASE_REQ.2 Abgeleitete Sicherheitsanforderungen            |
|                                         | ASE_SPD.1 Sicherheitsproblemdefinition                    |
|                                         | ASE_TSS.1 Zusammenfassende Spezifikation des TOEs         |
| ATE: Tests                              | ATE_COV.1 Nachweis der Abdeckung                          |
|                                         | ATE_FUN.1 Funktionsprüfung                                |
|                                         | ATE_IND.2 Unabhängige Prüfungen – Stichprobe              |
| AVA: Anfälligkeitsbewertung             | AVA_VAN.2 Anfälligkeitsanalyse                            |

## 7.5 Vertrauenswürdigkeitsstufe 3 (EAL3) – methodisch geprüft und überprüft

### 7.5.1 Ziele

EAL3 erlaubt einem gewissenhaften Entwickler das Erreichen höchster Vertrauenswürdigkeit durch positives Sicherheits-Engineering während der Designphase ohne eine wesentliche Veränderung sachgerechter Entwicklungspraktiken.

EAL3 ist für Situationen anwendbar, in denen Entwickler oder Benutzer einen moderaten Grad an unabhängig zugesicherter Sicherheit und eine gründliche Untersuchung des TOEs und seiner Entwicklung ohne wesentliches Re-Engineering erfordern.

### 7.5.2 Vertrauenswürdigkeitskomponenten

**EAL3** bietet Vertrauenswürdigkeit durch eine vollständige Sicherheitsvorgabe und durch eine Analyse der SFRs in dieser ST unter Verwendung einer Funktions- und Schnittstellenspezifikation, einer Leitliniendokumentation und **einer architektonischen** Beschreibung des TOE-**Designs**, um das Sicherheitsverhalten zu verstehen.

Die Analyse wird unterstützt durch unabhängige Prüfung der TSF, durch Nachweis der Entwicklerprüfung auf Grundlage der Funktionsspezifikation **und des TOE-Designs**, durch ausgewählte unabhängige Bestätigung der Prüfergebnisse des Entwicklers sowie durch eine Anfälligkeitsanalyse (auf Grundlage von Funktionsspezifikation, TOE-Design, Beschreibung der Sicherheitsarchitektur und bereitgestelltem Nachweis der Leitlinien), die die Widerstandsfähigkeit gegen eindringende Angreifer mit grundlegendem Angriffspotential nachweist.

**EAL3** bietet außerdem Vertrauenswürdigkeit durch **die** Verwendung von **Kontrollen der Entwicklungsumgebung**, durch **TOE-Konfigurationsmanagement** und durch Nachweis von sicheren Lieferverfahren.

Diese EAL-Stufe ist eine sinnvolle Zunahme der Vertrauenswürdigkeit im Vergleich zu **EAL2** durch die Forderung nach **vollständigerer Abdeckung** der Prüfung der **Sicherheitsfunktionalität** und nach **Mechanismen und/oder Verfahren, die ein gewisses Vertrauen bieten, dass der TOE während der Entwicklung nicht manipuliert wird.**

**Tabelle 4 — EAL3**

| Vertrauenswürdigkeitsklasse             | Vertrauenswürdigkeitskomponenten                                   |
|-----------------------------------------|--------------------------------------------------------------------|
| ADV: Entwicklung                        | ADV_ARC.1 Beschreibung der Sicherheitsarchitektur                  |
|                                         | ADV_FSP.3 Funktionsspezifikation mit vollständiger Zusammenfassung |
|                                         | ADV_TDS.2 Architekturdesign                                        |
| AGD: Leitliniendokumente                | AGD_OPE.1 Operative Leitlinien für Benutzer                        |
|                                         | AGD_PRE.1 Vorbereitende Verfahren                                  |
| ALC: Unterstützung des Lebenszyklus     | ALC_CMC.3 Autorisierungskontrollen                                 |
|                                         | ALC_CMS.3 CM-Abdeckung für die Darstellung der Implementierung     |
|                                         | ALC_DEL.1 Lieferverfahren                                          |
|                                         | ALC_DVS.1 Identifikation von Sicherheitsmaßnahmen                  |
|                                         | ALC_LCD.1 Vom Entwickler definiertes Lebenszyklusmodell            |
| ASE: Evaluierung der Sicherheitsvorgabe | ASE_CCL.1 Konformitätsansprüche                                    |
|                                         | ASE_ECD.1 Erweiterte Komponentendefinition                         |
|                                         | ASE_INT.1 ST Einleitung                                            |
|                                         | ASE_OBJ.2 Sicherheitszielsetzungen                                 |
|                                         | ASE_REQ.2 Abgeleitete Sicherheitsanforderungen                     |
|                                         | ASE_SPD.1 Sicherheitsproblemdefinition                             |
|                                         | ASE_TSS.1 Zusammenfassende Spezifikation des TOEs                  |
| ATE: Tests                              | ATE_COV.2 Analyse der Abdeckung                                    |
|                                         | ATE_DPT.1 Prüfung: grundlegendes Design                            |
|                                         | ATE_FUN.1 Funktionsprüfung                                         |
|                                         | ATE_IND.2 Unabhängige Prüfungen – Stichprobe                       |
| AVA: Anfälligkeitsbewertung             | AVA_VAN.2 Anfälligkeitsanalyse                                     |

## 7.6 Vertrauenswürdigkeitsstufe 4 (EAL4) – methodisch entwickelt, geprüft und überprüft

### 7.6.1 Ziele

EAL4 erlaubt einem Entwickler das Erreichen höchster Vertrauenswürdigkeit durch positives Sicherheits-Engineering auf Grundlage sachgerechter Entwicklungspraktiken, die trotz ihrer Strenge kein wesentliches Fachwissen, besondere Fähigkeiten oder andere Ressourcen erfordern. EAL4 ist die höchste Stufe, bei der eine Nachrüstung einer bestehenden Produktlinie wahrscheinlich noch betriebswirtschaftlich praktikabel ist.

EAL4 ist damit für Situationen anwendbar, in denen Entwickler oder Benutzer einen moderaten bis hohen Grad an unabhängig zugesicherter Sicherheit bei handelsüblichen TOEs erfordern und auf zusätzlich anfallende Kosten für das Sicherheits-Engineering vorbereitet sind.

### 7.6.2 Vertrauenswürdigkeitskomponenten

**EAL4** bietet Vertrauenswürdigkeit durch eine vollständige Sicherheitsvorgabe und durch eine Analyse der SFRs in dieser ST unter Verwendung einer Funktionsspezifikation und einer **vollständigen** Schnittstellenspezifikation, einer Leitliniendokumentation, **einer** Beschreibung des **grundlegenden modularen** TOE-Designs **sowie einer Teilmenge der Implementierung**, um das Sicherheitsverhalten zu verstehen.

Die Analyse wird unterstützt durch unabhängige Prüfung der TSF, durch Nachweis der Entwicklerprüfung auf Grundlage der Funktionsspezifikation und des TOE-Designs, durch ausgewählte unabhängige Bestätigung der Prüfergebnisse des Entwicklers sowie durch eine Anfälligkeitsanalyse (auf Grundlage von Funktionsspezifikation, TOE-Design, **Darstellung der Implementierung**, Beschreibung der Sicherheitsarchitektur und bereitgestelltem Nachweis der Leitlinien), die die Widerstandsfähigkeit gegen eindringende Angreifer mit **einem erweitert- grundlegenden** Angriffspotential nachweist.

**EAL4** bietet außerdem Vertrauenswürdigkeit durch die Verwendung von Kontrollen der Entwicklungsumgebung **und durch zusätzliches** TOE-Konfigurationsmanagement **einschließlich Automatisierung** sowie durch Nachweis von sicheren Lieferverfahren.

Diese EAL-Stufe ist eine sinnvolle Zunahme der Vertrauenswürdigkeit im Vergleich zu **EAL3** durch die Forderung nach umfangreicherer **Beschreibung des Designs**, nach der **Darstellung der Implementierung für die gesamte TSF** und nach **verbesserten** Mechanismen und/oder Verfahren, die Vertrauen bieten, dass der TOE während der Entwicklung nicht manipuliert wird.

**Tabelle 5 — EAL4**

| Vertrauenswürdigkeitsklasse         | Vertrauenswürdigkeitskomponenten                                          |
|-------------------------------------|---------------------------------------------------------------------------|
| ADV: Entwicklung                    | ADV_ARC.1 Beschreibung der Sicherheitsarchitektur                         |
|                                     | ADV_FSP.4 Vollständige Funktionsspezifikation                             |
|                                     | ADV_IMP.1 Darstellung der Implementierung der TSF                         |
|                                     | ADV_TDS.3 Grundsätzliches modulares Design                                |
| AGD: Leitliniendokumente            | AGD_OPE.1 Operative Leitlinien für Benutzer                               |
|                                     | AGD_PRE.1 Vorbereitende Verfahren                                         |
| ALC: Unterstützung des Lebenszyklus | ALC_CMC.4 Herstellungsunterstützung, Abnahmeverfahren und Automatisierung |
|                                     | ALC_CMS.4 CM-Abdeckung für die Problemverfolgung                          |
|                                     | ALC_DEL.1 Lieferverfahren                                                 |
|                                     | ALC_DVS.1 Identifikation von Sicherheitsmaßnahmen                         |
|                                     | ALC_LCD.1 Vom Entwickler definiertes Lebenszyklusmodell                   |
|                                     | ALC_TAT.1 Genau festgelegte Entwicklungswerkzeuge                         |

| Vertrauenswürdigkeitsklasse             | Vertrauenswürdigkeitskomponenten                  |
|-----------------------------------------|---------------------------------------------------|
| ASE: Evaluierung der Sicherheitsvorgabe | ASE_CCL.1 Konformitätsansprüche                   |
|                                         | ASE_ECD.1 Erweiterte Komponentendefinition        |
|                                         | ASE_INT.1 ST Einleitung                           |
|                                         | ASE_OBJ.2 Sicherheitszielsetzungen                |
|                                         | ASE_REQ.2 Abgeleitete Sicherheitsanforderungen    |
|                                         | ASE_SPD.1 Sicherheitsproblemdefinition            |
|                                         | ASE_TSS.1 Zusammenfassende Spezifikation des TOEs |
| ATE: Tests                              | ATE_COV.2 Analyse der Abdeckung                   |
|                                         | ATE_DPT.1 Prüfung: grundlegendes Design           |
|                                         | ATE_FUN.1 Funktionsprüfung                        |
|                                         | ATE_IND.2 Unabhängige Prüfungen – Stichprobe      |
| AVA: Anfälligkeitsbewertung             | AVA_VAN.3 Konzentrierte Anfälligkeitsanalyse      |

## 7.7 Vertrauenswürdigkeitsstufe 5 (EAL5) – semiformal entwickelt und geprüft

### 7.7.1 Ziele

EAL5 erlaubt einem Entwickler das Erreichen höchster Vertrauenswürdigkeit durch Sicherheits-Engineering auf Grundlage strenger Entwicklungspraktiken, die von moderater Anwendung fachgerechter Sicherheits-Engineering-Techniken unterstützt werden. Ein solches TOE wird vermutlich mit der Absicht zur Erreichung der EAL5-Vertrauenswürdigkeit konzipiert und entwickelt. Es ist wahrscheinlich, dass die zusätzlichen Kosten, die den EAL5-Anforderungen zurechenbar sind, relativ zu einer strengen Entwicklung ohne Anwendung der fachgerechten Techniken nicht hoch sein werden.

EAL5 ist anwendbar für Situationen, in denen Entwickler oder Benutzer einen hohen Grad an unabhängig zugesicherter Sicherheit bei einer geplanten Entwicklung erfordern und einen strengen Entwicklungsansatz ohne unangemessene Kosten für fachgerechte Sicherheits-Engineering-Techniken erfordern.

### 7.7.2 Vertrauenswürdigkeitskomponenten

**EAL5** bietet Vertrauenswürdigkeit durch eine vollständige Sicherheitsvorgabe und durch eine Analyse der SFRs in dieser ST unter Verwendung einer Funktionsspezifikation und einer vollständigen Schnittstellenspezifikation, einer Leitliniendokumentation, einer Beschreibung des TOE-Designs sowie der Implementierung, um das Sicherheitsverhalten zu verstehen. **Ein modulares TSF-Design ist ebenfalls erforderlich.**

Die Analyse wird unterstützt durch unabhängige Prüfung der TSF, durch Nachweis der Entwicklerprüfung auf Grundlage der Funktionsspezifikation und des TOE-Designs, durch ausgewählte unabhängige Bestätigung der Prüfergebnisse des Entwicklers sowie durch **eine unabhängige** Anfälligkeitsanalyse, die die Widerstandsfähigkeit gegen eindringende Angreifer mit **einem moderaten** Angriffspotential nachweist.

**EAL5** bietet außerdem Vertrauenswürdigkeit durch die Verwendung von Kontrollen der Entwicklungs-umgebung und durch **umfangreiches** TOE-Konfigurationsmanagement, einschließlich Automatisierung, sowie durch Nachweis von sicheren Lieferverfahren.

Diese EAL-Stufe ist eine sinnvolle Zunahme der Vertrauenswürdigkeit im Vergleich zu **EAL4** durch die Forderung nach **semiformaler Beschreibung des Designs, nach einer strukturierten (und somit analysierbaren) Architektur** und nach verbesserten Mechanismen und/oder Verfahren, die Vertrauen bieten, dass der TOE während der Entwicklung nicht manipuliert wird.

**Tabelle 6 — EAL5**

| Vertrauenswürdigkeitsklasse             | Vertrauenswürdigkeitskomponenten                                                               |
|-----------------------------------------|------------------------------------------------------------------------------------------------|
| ADV: Entwicklung                        | ADV_ARC.1 Beschreibung der Sicherheitsarchitektur                                              |
|                                         | ADV_FSP.5 Vollständige semiformale Funktionsspezifikation mit zusätzlichen Fehlerinformationen |
|                                         | ADV_IMP.1 Darstellung der Implementierung der TSF                                              |
|                                         | ADV_INT.2 Wohlstrukturierte Interna                                                            |
|                                         | ADV_TDS.4 Semiformales modulares Design                                                        |
| AGD: Leitliniendokumente                | AGD_OPE.1 Operative Leitlinien für Benutzer                                                    |
|                                         | AGD_PRE.1 Vorbereitende Verfahren                                                              |
| ALC: Unterstützung des Lebenszyklus     | ALC_CMC.4 Herstellungsunterstützung, Abnahmeverfahren und Automatisierung                      |
|                                         | ALC_CMS.5 CM Abdeckung für Entwicklungswerkzeuge                                               |
|                                         | ALC_DEL.1 Lieferverfahren                                                                      |
|                                         | ALC_DVS.1 Identifikation von Sicherheitsmaßnahmen                                              |
|                                         | ALC_LCD.1 Vom Entwickler definiertes Lebenszyklusmodell                                        |
|                                         | ALC_TAT.2 Konformität mit Implementierungsstandards                                            |
| ASE: Evaluierung der Sicherheitsvorgabe | ASE_CCL.1 Konformitätsansprüche                                                                |
|                                         | ASE_ECD.1 Erweiterte Komponentendefinition                                                     |
|                                         | ASE_INT.1 ST Einleitung                                                                        |
|                                         | ASE_OBJ.2 Sicherheitszielsetzungen                                                             |
|                                         | ASE_REQ.2 Abgeleitete Sicherheitsanforderungen                                                 |
|                                         | ASE_SPD.1 Sicherheitsproblemdefinition                                                         |
|                                         | ASE_TSS.1 Zusammenfassende Spezifikation des TOEs                                              |
| ATE: Tests                              | ATE_COV.2 Analyse der Abdeckung                                                                |
|                                         | ATE_DPT.3 Prüfung: modulares Design                                                            |
|                                         | ATE_FUN.1 Funktionsprüfung                                                                     |
|                                         | ATE_IND.2 Unabhängige Prüfungen – Stichprobe                                                   |
| AVA: Anfälligkeitsbewertung             | AVA_VAN.4 Methodische Anfälligkeitsanalyse                                                     |

## 7.8 Vertrauenswürdigkeitsstufe 6 (EAL6) – semiformal verifiziertes Design und geprüft

### 7.8.1 Ziele

EAL6 erlaubt einem Entwickler das Erreichen hoher Vertrauenswürdigkeit durch Anwendung von Sicherheits-Engineering-Techniken für eine strenge Entwicklungsumgebung zur Herstellung eines hochwertigen TOEs zum Schutz hochwertiger Vermögenswerte vor erheblichen Risiken.

EAL6 ist daher für die Entwicklung von Sicherheits-TOEs für Anwendungen in sehr riskanten Situationen anwendbar, in denen der Wert der geschützten Vermögenswerte die zusätzlichen Kosten rechtfertigt.

## 7.8.2 Vertrauenswürdigkeitskomponenten

**EAL6** bietet Vertrauenswürdigkeit durch eine vollständige Sicherheitsvorgabe und durch eine Analyse der SFRs in dieser ST unter Verwendung einer Funktionsspezifikation und einer vollständigen Schnittstellenspezifikation, einer Leitliniendokumentation, des TOE-Designs sowie der Implementierung, um das Sicherheitsverhalten zu verstehen. **Vertrauenswürdigkeit wird zusätzlich über ein formales Modell an ausgewählten TOE-Sicherheitspolitiken und eine semiformale Darstellung der Funktionsspezifikation und des TOE-Designs erreicht.** Ein modulares, **geschichtetes und einfaches** TSF-Design ist ebenfalls erforderlich.

Die Analyse wird unterstützt durch unabhängige Prüfung der TSF, durch Nachweis der Entwicklerprüfung auf Grundlage der Funktionsspezifikation und des TOE-Designs, durch ausgewählte unabhängige Bestätigung der Prüfergebnisse des Entwicklers sowie durch eine unabhängige Anfälligkeitsanalyse, die die Widerstandsfähigkeit gegen eindringende Angreifer mit einem **hohen** Angriffspotential nachweist.

**EAL6** bietet außerdem Vertrauenswürdigkeit durch die Verwendung eines **strukturierten Entwicklungsprozesses**, durch Kontrollen der **Entwicklungsumgebung** und durch umfangreiches TOE-Konfigurationsmanagement einschließlich **vollständiger** Automatisierung sowie durch Nachweis von sicheren Lieferverfahren.

Diese EAL-Stufe ist eine sinnvolle Zunahme der Vertrauenswürdigkeit im Vergleich zu **EAL5** durch die Forderung nach **umfangreicherer Analyse**, nach einer **strukturierten Darstellung der Implementierung**, nach aufwendigerer **architektonischer Struktur (z. B. Schichtung)**, nach **umfangreicherer unabhängiger Anfälligkeitsanalyse** und nach Verbesserungen bei **Konfigurationsmanagement und Kontrollen** der Entwicklungsumgebung.

Tabelle 7 — EAL6

| Vertrauenswürdigkeitsklasse         | Vertrauenswürdigkeitskomponenten                                                               |
|-------------------------------------|------------------------------------------------------------------------------------------------|
| ADV: Entwicklung                    | ADV_ARC.1 Beschreibung der Sicherheitsarchitektur                                              |
|                                     | ADV_FSP.5 Vollständige semiformale Funktionsspezifikation mit zusätzlichen Fehlerinformationen |
|                                     | ADV_IMP.2 Vollständige Zuordnung der Darstellung der Implementierung der TSF                   |
|                                     | ADV_INT.3 Minimal komplexe Interna                                                             |
|                                     | ADV_SPM.1 Formales TOE Sicherheitspolitikmodell                                                |
|                                     | ADV_TDS.5 Vollständiges semiformales modulares Design                                          |
| AGD: Leitliniendokumente            | AGD_OPE.1 Operative Leitlinien für Benutzer                                                    |
|                                     | AGD_PRE.1 Vorbereitende Verfahren                                                              |
| ALC: Unterstützung des Lebenszyklus | ALC_CMC.5 Erweiterte Unterstützung                                                             |
|                                     | ALC_CMS.5 CM Abdeckung für Entwicklungswerkzeuge                                               |
|                                     | ALC_DEL.1 Lieferverfahren                                                                      |
|                                     | ALC_DVS.2 Angemessenheit von Sicherheitsmaßnahmen                                              |
|                                     | ALC_LCD.1 Vom Entwickler definiertes Lebenszyklusmodell                                        |
|                                     | ALC_TAT.3 Konformität mit Implementierungsstandards – alle Teile                               |

| Vertrauenswürdigkeitsklasse             | Vertrauenswürdigkeitskomponenten                      |
|-----------------------------------------|-------------------------------------------------------|
| ASE: Evaluierung der Sicherheitsvorgabe | ASE_CCL.1 Konformitätsansprüche                       |
|                                         | ASE_ECD.1 Erweiterte Komponentendefinition            |
|                                         | ASE_INT.1 ST Einleitung                               |
|                                         | ASE_OBJ.2 Sicherheitszielsetzungen                    |
|                                         | ASE_REQ.2 Abgeleitete Sicherheitsanforderungen        |
|                                         | ASE_SPD.1 Sicherheitsproblemdefinition                |
|                                         | ASE_TSS.1 Zusammenfassende Spezifikation des TOEs     |
| ATE: Tests                              | ATE_COV.3 Strenge Analyse der Abdeckung               |
|                                         | ATE_DPT.3 Prüfung: modulares Design                   |
|                                         | ATE_FUN.2 Geordnete Funktionsprüfung                  |
|                                         | ATE_IND.2 Unabhängige Prüfungen – Stichprobe          |
| AVA: Anfälligkeitsbewertung             | AVA_VAN.5 Erweiterte methodische Anfälligkeitsanalyse |

## 7.9 Vertrauenswürdigkeitsstufe 7 (EAL7) – formal verifiziertes Design und geprüft

### 7.9.1 Ziele

EAL7 ist für die Entwicklung von Sicherheits-TOEs für Anwendungen in äußerst hochriskanten Situationen anwendbar und/oder wenn der hohe Wert der Vermögenswerte die hohen Kosten rechtfertigt. Praktische Anwendungen von EAL7 sind aktuell begrenzt auf TOEs mit engem Schwerpunkt auf Sicherheitsfunktionalität, die für umfangreiche formale Analyse zugänglich sind.

### 7.9.2 Vertrauenswürdigkeitskomponenten

**EAL7** bietet Vertrauenswürdigkeit durch eine vollständige Sicherheitsvorgabe und durch eine Analyse der SFRs in dieser ST unter Verwendung einer Funktionsspezifikation und einer vollständigen Schnittstellenspezifikation, einer Leitliniendokumentation, des TOE-Designs sowie **einer strukturierten Darstellung der Implementierung**, um das Sicherheitsverhalten zu verstehen. Vertrauenswürdigkeit wird zusätzlich über ein formales Modell an ausgewählten TOE-Sicherheitspolitiken und eine semiformale Darstellung der Funktionsspezifikation und des TOE-Designs erreicht. Ein modulares, geschichtetes und einfaches TSF-Design ist ebenfalls erforderlich.

Die Analyse wird unterstützt durch unabhängige Prüfung der TSF, durch Nachweis der Entwicklerprüfung auf Grundlage der Funktionsspezifikation, des TOE-Designs **und der Darstellung der Implementierung, durch vollständige** unabhängige Bestätigung der Prüfergebnisse des Entwicklers sowie durch eine unabhängige Anfälligkeitsanalyse, die die Widerstandsfähigkeit gegen eindringende Angreifer mit einem hohen Angriffspotential nachweist.

**EAL7** bietet außerdem Vertrauenswürdigkeit durch die Verwendung eines strukturierten Entwicklungsprozesses, durch Kontrollen der Entwicklungsumgebung und durch umfangreiches TOE-Konfigurationsmanagement, einschließlich vollständiger Automatisierung, sowie durch Nachweis von sicheren Lieferverfahren.

Diese EAL-Stufe ist eine sinnvolle Zunahme der Vertrauenswürdigkeit im Vergleich zu **EAL6** durch die Forderung nach umfangreichere Analyse **unter Verwendung formaler Repräsentationen** und **formaler Korrespondenz** sowie **nach umfangreicher Prüfung**.

**Tabelle 8 — EAL7**

| Vertrauenswürdigkeitsklasse             | Vertrauenswürdigkeitskomponenten                                                                  |
|-----------------------------------------|---------------------------------------------------------------------------------------------------|
| ADV: Entwicklung                        | ADV_ARC.1 Beschreibung der Sicherheitsarchitektur                                                 |
|                                         | ADV_FSP.6 Vollständige semiformale Funktionsspezifikation mit zusätzlicher formaler Spezifikation |
|                                         | ADV_IMP.2 Vollständige Zuordnung der Darstellung der Implementierung der TSF                      |
|                                         | ADV_INT.3 Minimal komplexe Interna                                                                |
|                                         | ADV_SPM.1 Formales TOE Sicherheitspolitikmodell                                                   |
|                                         | ADV_TDS.6 Vollständiges semiformales modulares Design mit formaler allgemeiner Designdarstellung  |
| AGD: Leitliniendokumente                | AGD_OPE.1 Operative Leitlinien für Benutzer                                                       |
|                                         | AGD_PRE.1 Vorbereitende Verfahren                                                                 |
| ALC: Unterstützung des Lebenszyklus     | ALC_CMC.5 Erweiterte Unterstützung                                                                |
|                                         | ALC_CMS.5 CM Abdeckung für Entwicklungswerkzeuge                                                  |
|                                         | ALC_DEL.1 Lieferverfahren                                                                         |
|                                         | ALC_DVS.2 Angemessenheit von Sicherheitsmaßnahmen                                                 |
|                                         | ALC_LCD.2 Messbares Lebenszyklusmodell                                                            |
|                                         | ALC_TAT.3 Konformität mit Implementierungsstandards – alle Teile                                  |
| ASE: Evaluierung der Sicherheitsvorgabe | ASE_CCL.1 Konformitätsansprüche                                                                   |
|                                         | ASE_ECD.1 Erweiterte Komponentendefinition                                                        |
|                                         | ASE_INT.1 ST Einleitung                                                                           |
|                                         | ASE_OBJ.2 Sicherheitszielsetzungen                                                                |
|                                         | ASE_REQ.2 Abgeleitete Sicherheitsanforderungen                                                    |
|                                         | ASE_SPD.1 Sicherheitsproblemdefinition                                                            |
|                                         | ASE_TSS.1 Zusammenfassende Spezifikation des TOEs                                                 |
| ATE: Tests                              | ATE_COV.3 Strenge Analyse der Abdeckung                                                           |
|                                         | ATE_DPT.4 Prüfung: Darstellung der Implementierung                                                |
|                                         | ATE_FUN.2 Geordnete Funktionsprüfung                                                              |
|                                         | ATE_IND.3 Unabhängige Prüfungen – vollständig                                                     |
| AVA: Anfälligkeitsbewertung             | AVA_VAN.5 Erweiterte methodische Anfälligkeitsanalyse                                             |

## 8 Zusammengesetzte Sicherheitspakete

Die zusammengesetzten Sicherheitspakete (CAPs) stellen eine ansteigende Skala für zusammengesetzte TOEs dar, bei der der Grad der erreichbaren Vertrauenswürdigkeit mit den damit verbundenen Kosten und der Durchführbarkeit abgewogen wird.

Es ist wichtig darauf hinzuweisen, dass nur eine geringe Anzahl an Familien und Komponenten aus diesem Teil von ISO/IEC 15408 in den CAPs enthalten sind. Das liegt am Wesen des Erstellens auf Grundlage der

Evaluierungsergebnisse zuvor evaluierter Entitäten (Basiskomponenten und abhängige Komponenten) und bedeutet nicht, dass diese keine sinnvolle und erstrebenswerte Vertrauenswürdigkeit bieten.

## 8.1 Übersicht über die zusammengesetzten Sicherheitspakete (CAPs)

CAPs sind für zusammengesetzte TOEs vorgesehen, die aus Komponenten bestehen, die eine Komponenten-TOE-Evaluierung durchlaufen haben (oder derzeit durchlaufen); siehe Anhang B. Die einzelnen Komponenten werden für eine EAL-Stufe oder ein anderes in der ST spezifiziertes Sicherheitspaket zertifiziert worden sein. Es wird erwartet, dass ein grundlegender Grad an Vertrauenswürdigkeit in einem zusammengesetzten TOE durch die Anwendung von EAL1 erreicht wird, was durch allgemein öffentlich verfügbare Informationen über die Komponenten erreicht werden kann. (EAL1 kann wie hier angegeben für Komponenten-TOEs und zusammengesetzte TOEs angewendet werden.) CAPs bieten einen alternativen Ansatz zum Erlangen höherer Vertrauenswürdigkeitsgrade für ein zusammengesetztes TOE als die Anwendung der EAL-Stufen oberhalb EAL1.

Obwohl eine abhängige Komponente unter Verwendung einer bereits evaluierten und zertifizierten Basiskomponente evaluiert werden kann, um die IT-Plattformanforderungen in der Umgebung zu erfüllen, bietet dies keine formale Vertrauenswürdigkeit für die Interaktionen zwischen den Komponenten oder die mögliche Einführung von aus ihrer Zusammensetzung resultierenden Anfälligkeiten. Zusammengesetzte Sicherheitspakete berücksichtigen diese Interaktionen und stellen bei höheren Graden der Vertrauenswürdigkeit sicher, dass die Schnittstelle zwischen den Komponenten auch selbst das Subjekt der Prüfung war. Eine Anfälligkeitsanalyse des zusammengesetzten TOEs wird ebenfalls durchgeführt, um die mögliche Einführung von Anfälligkeiten durch die Zusammensetzung der Komponenten zu berücksichtigen.

Tabelle 9 zeigt eine Zusammenfassung der CAPs. Die Spalten stellen eine hierarchisch geordnete Reihe von CAPs dar, während die Zeilen die Vertrauenswürdigkeitsfamilien zeigen. Jede Ziffer in der sich ergebenden Matrix bezeichnet gegebenenfalls eine bestimmte Vertrauenswürdigkeitskomponente.

Wie im folgenden Unterabschnitt dargelegt, sind zur Bewertung der Vertrauenswürdigkeit eines TOEs drei hierarchisch geordnete zusammengesetzte Sicherheitspakete in von ISO/IEC 15408 definiert. Sie sind insofern hierarchisch geordnet, dass jedes CAP eine größere Vertrauenswürdigkeit darstellt als alle niedrigeren CAPs. Die Zunahme der Vertrauenswürdigkeit von CAP zu CAP wird durch den Austausch einer hierarchisch höheren Vertrauenswürdigkeitskomponente derselben Vertrauenswürdigkeitsfamilie (d. h. zunehmende Strenge, Umfang und/oder Tiefe) und durch das Hinzufügen von Vertrauenswürdigkeitskomponenten aus anderen Vertrauenswürdigkeitsfamilien (d. h. Hinzufügen neuer Anforderungen) erreicht. Diese Zunahmen führen zu einer umfangreicheren Analyse der Zusammensetzung, um die Auswirkung auf die für die einzelnen Komponenten-TOEs gewonnenen Evaluierungsergebnisse zu identifizieren.

Diese CAPs bestehen aus einer geeigneten Kombination aus Vertrauenswürdigkeitskomponenten, die in Abschnitt 6 dieses Teils von ISO/IEC 15408 beschrieben sind. Genauer ausgedrückt enthält jedes CAP nicht mehr als eine Komponente jeder Vertrauenswürdigkeitsfamilie und alle Abhängigkeiten zur Vertrauenswürdigkeit jeder Komponente werden angesprochen.

Die CAPs berücksichtigen nur die Widerstandsfähigkeit gegen einen Angreifer mit einem Angriffspotential bis erweitert-grundlegend. Das liegt am Grad der Designinformationen, die über ACO\_DEV bereitgestellt werden können, was einige mit dem Angriffspotential verbundene Faktoren einschränkt (Kenntnis des zusammengesetzten TOEs) und folglich die Strenge der Anfälligkeitsanalyse beeinflusst, die vom Evaluator durchgeführt werden kann. Deshalb ist der Grad an Vertrauenswürdigkeit im zusammengesetzten TOE begrenzt, obwohl die Vertrauenswürdigkeit der einzelnen Komponenten im zusammengesetzten TOE wesentlich höher sein kann.

**Tabelle 9 — Zusammenfassung der zusammengesetzten Sicherheitspakete**

| Vertrauenswürdigkeits-<br>klasse      | Vertrauenswürdigkeits-<br>familie | Vertrauenswürdigkeitskomponenten nach<br>zusammengesetztem Sicherheitspaket |       |       |
|---------------------------------------|-----------------------------------|-----------------------------------------------------------------------------|-------|-------|
|                                       |                                   | CAP-A                                                                       | CAP-B | CAP-C |
| Zusammensetzung                       | ACO_COR                           | 1                                                                           | 1     | 1     |
|                                       | ACO_CTT                           | 1                                                                           | 2     | 2     |
|                                       | ACO_DEV                           | 1                                                                           | 2     | 3     |
|                                       | ACO_REL                           | 1                                                                           | 1     | 2     |
|                                       | ACO_VUL                           | 1                                                                           | 2     | 3     |
| Leitliniendokumente                   | AGD_OPE                           | 1                                                                           | 1     | 1     |
|                                       | AGD_PRE                           | 1                                                                           | 1     | 1     |
| Lebenszyklus-<br>unterstützung        | ALC_CMC                           | 1                                                                           | 1     | 1     |
|                                       | ALC_CMS                           | 2                                                                           | 2     | 2     |
|                                       | ALC_DEL                           |                                                                             |       |       |
|                                       | ALC_DVS                           |                                                                             |       |       |
|                                       | ALC_FLR                           |                                                                             |       |       |
|                                       | ALC_LCD                           |                                                                             |       |       |
|                                       | ALC_TAT                           |                                                                             |       |       |
| Evaluierung der<br>Sicherheitsvorgabe | ASE_CCL                           | 1                                                                           | 1     | 1     |
|                                       | ASE_ECD                           | 1                                                                           | 1     | 1     |
|                                       | ASE_INT                           | 1                                                                           | 1     | 1     |
|                                       | ASE_OBJ                           | 1                                                                           | 2     | 2     |
|                                       | ASE_REQ                           | 1                                                                           | 2     | 2     |
|                                       | ASE_SPD                           |                                                                             | 1     | 1     |
|                                       | ASE_TSS                           | 1                                                                           | 1     | 1     |

## 8.2 Einzelheiten zusammengesetzter Sicherheitspakete

Die folgenden Unterabschnitte enthalten Definitionen zu den CAPs und heben Unterschiede zwischen den einzelnen Anforderungen und den Merkmalen dieser Anforderungen über Fettmarkierung hervor.

## 8.3 Zusammengesetztes Sicherheitspaket A (CAP-A) – strukturell zusammengesetzt

### 8.3.1 Ziele

CAP-A ist anwendbar, wenn ein zusammengesetztes TOE integriert wird und Vertrauen in die korrekten Sicherheitsmaßnahmen der entstehenden Zusammensetzung erforderlich ist. Dies erfordert die Kooperation des Entwicklers der abhängigen Komponente hinsichtlich der Bereitstellung von Designinformationen und Prüfergebnissen aus der Zertifizierung der abhängigen Komponente, ohne dabei die Beteiligung des Entwicklers der Basiskomponente zu benötigen.

CAP-A ist damit anwendbar für Situationen, in denen Entwickler oder Benutzer einen geringen oder moderaten Grad an unabhängig zugesicherter Sicherheit ohne unmittelbare Verfügbarkeit der vollständigen Entwicklungshistorie erfordern.

### 8.3.2 Vertrauenswürdigkeitskomponenten

CAP-A bietet Vertrauenswürdigkeit durch die Analyse einer Sicherheitsvorgabe für den zusammengesetzten TOE. Die SFRs in der ST des zusammengesetzten TOEs werden unter Verwendung der Evaluierungsergebnisse der Komponenten-TOEs (z. B. ST, Leitliniendokumentation) und einer Spezifikation der Schnittstellen zwischen den Komponenten-TOEs im zusammengesetzten TOE analysiert, um ein Verständnis für das Sicherheitsverhalten zu erlangen.

Die Analyse wird unterstützt durch unabhängige Prüfung der Schnittstellen der Basiskomponente, auf die sich die abhängige Komponente verlässt, entsprechend der Beschreibung in der Verlässlichkeitsinformation, durch den Nachweis der Entwicklerprüfung auf Grundlage der Verlässlichkeitsinformation, der Entwicklungsinformation und der Begründung der Zusammensetzung, sowie durch ausgewählte unabhängige Bestätigung der Prüfergebnisse des Entwicklers. Die Analyse wird außerdem durch eine Anfälligkeitsüberprüfung des zusammengesetzten TOEs durch den Evaluator unterstützt.

CAP-A bietet außerdem Vertrauenswürdigkeit durch eindeutige Identifikation des zusammengesetzten TOEs (d. h. IT-TOE- und Leitliniendokumentation).

Tabelle 10 — CAP-A

| Vertrauenswürdigkeitsklasse             | Vertrauenswürdigkeitskomponenten                            |
|-----------------------------------------|-------------------------------------------------------------|
| ACO: Zusammensetzung                    | ACO_COR.1 Begründung der Zusammensetzung                    |
|                                         | ACO_CTT.1 Schnittstellenprüfung                             |
|                                         | ACO_DEV.1 Funktionsbeschreibung                             |
|                                         | ACO_REL.1 Einfache Verlässlichkeitsinformation              |
|                                         | ACO_VUL.1 Anfälligkeitsüberprüfung der Zusammensetzung      |
| AGD: Leitliniendokumente                | AGD_OPE.1 Operative Leitlinien für Benutzer                 |
|                                         | AGD_PRE.1 Vorbereitende Verfahren                           |
| ALC: Unterstützung des Lebenszyklus     | ALC_CMC.1 Kennzeichnung des TOEs                            |
|                                         | ALC_CMS.2 CM Abdeckung für Teile des TOEs                   |
| ASE: Evaluierung der Sicherheitsvorgabe | ASE_CCL.1 Konformitätsansprüche                             |
|                                         | ASE_ECD.1 Erweiterte Komponentendefinition                  |
|                                         | ASE_INT.1 ST Einleitung                                     |
|                                         | ASE_OBJ.1 Sicherheitszielsetzungen für die Betriebsumgebung |
|                                         | ASE_REQ.1 Festgelegte Sicherheitsanforderungen              |
|                                         | ASE_TSS.1 Zusammenfassende Spezifikation des TOEs           |

## 8.4 Zusammengesetztes Sicherheitspaket B (CAP-B) – methodisch zusammengesetzt

### 8.4.1 Ziele

CAP-B erlaubt einem gewissenhaften Entwickler das Erreichen höchster Vertrauenswürdigkeit durch ein auf Teilsystemebene bestehendes Verständnis der Auswirkungen von Interaktionen zwischen im zusammengesetzten TOE integrierten Komponenten-TOEs und gleichzeitiger Minimierung der Notwendigkeit, den Entwickler der Basiskomponente zu beteiligen.

CAP-B ist für Situationen anwendbar, in denen Entwickler oder Benutzer einen moderaten Grad an unabhängig zugesicherter Sicherheit und eine gründliche Untersuchung des zusammengesetzten TOEs und seiner Entwicklung ohne wesentliches Re-Engineering erfordern.

#### 8.4.2 Vertrauenswürdigkeitskomponenten

**CAP-B** bietet Vertrauenswürdigkeit durch die Analyse einer **vollständigen** Sicherheitsvorgabe für den zusammengesetzten TOE. Die SFRs in der ST des zusammengesetzten TOEs werden unter Verwendung der Evaluierungsergebnisse der Komponenten-TOEs (z. B. ST, Leitliniendokumentation), einer Spezifikation der Schnittstellen zwischen den Komponenten-TOEs **und des TOE-Designs (mit Beschreibung der TSF-Teilsysteme)** in den **Entwicklungsinformationen** des zusammengesetzten TOEs analysiert, um ein Verständnis für das Sicherheitsverhalten zu erlangen.

Die Analyse wird unterstützt durch unabhängige Prüfung der Schnittstellen der Basiskomponente, auf die sich die abhängige Komponente verlässt, entsprechend der Beschreibung in der Verlässlichkeitsinformation (**nun auch einschließlich TOE-Design**), durch den Nachweis der Entwicklerprüfung auf Grundlage der Verlässlichkeitsinformation, der Entwicklungsinformation und der Begründung der Zusammensetzung, sowie durch ausgewählte unabhängige Bestätigung der Prüfergebnisse des Entwicklers. Die Analyse wird außerdem durch eine Anfälligkeitsanalyse des zusammengesetzten TOEs durch den Evaluator unterstützt, **die den Nachweis der Widerstandsfähigkeit gegen Angreifer mit grundlegendem Angriffspotential erbringt.**

**Dieses CAP ist eine sinnvolle Zunahme der Vertrauenswürdigkeit im Vergleich zu CAP-A durch die Forderung nach vollständigerer Abdeckung der Prüfung der Sicherheitsfunktionalität.**

**Tabelle 11 — CAP-B**

| Vertrauenswürdigkeitsklasse             | Vertrauenswürdigkeitskomponenten                   |
|-----------------------------------------|----------------------------------------------------|
| ACO: Zusammensetzung                    | ACO_COR.1 Begründung der Zusammensetzung           |
|                                         | ACO_CTT.2 Strenge Schnittstellenprüfung            |
|                                         | ACO_DEV.2 Einfacher Nachweis des Designs           |
|                                         | ACO_REL.1 Einfache Verlässlichkeitsinformation     |
|                                         | ACO_VUL.2 Anfälligkeitsanalyse der Zusammensetzung |
| AGD: Leitliniendokumente                | AGD_OPE.1 Operative Leitlinien für Benutzer        |
|                                         | AGD_PRE.1 Vorbereitende Verfahren                  |
| ALC: Unterstützung des Lebenszyklus     | ALC_CMC.1 Kennzeichnung des TOEs                   |
|                                         | ALC_CMS.2 CM Abdeckung für Teile des TOEs          |
| ASE: Evaluierung der Sicherheitsvorgabe | ASE_CCL.1 Konformitätsansprüche                    |
|                                         | ASE_ECD.1 Erweiterte Komponentendefinition         |
|                                         | ASE_INT.1 ST Einleitung                            |
|                                         | ASE_OBJ.2 Sicherheitszielsetzungen                 |
|                                         | ASE_REQ.2 Abgeleitete Sicherheitsanforderungen     |
|                                         | ASE_SPD.1 Sicherheitsproblemdefinition             |
|                                         | ASE_TSS.1 Zusammenfassende Spezifikation des TOEs  |

## 8.5 Zusammengesetztes Sicherheitspaket C (CAP-C) – methodisch zusammengesetzt, geprüft und überprüft

### 8.5.1 Ziele

CAP-C erlaubt einem Entwickler das Erreichen höchster Vertrauenswürdigkeit durch positive Analyse der Interaktionen zwischen den Komponenten des zusammengesetzten TOEs, die trotz Strenge keinen vollständigen Zugriff auf alle Evaluierungsnachweise der Basiskomponente erfordert.

CAP-C ist damit für Situationen anwendbar, in denen Entwickler oder Benutzer einen moderaten bis hohen Grad an unabhängig zugesicherter Sicherheit bei handelsüblichen zusammengesetzten TOEs erfordern und auf zusätzlich anfallende Kosten für das Sicherheits-Engineering vorbereitet sind.

### 8.5.2 Vertrauenswürdigkeitskomponenten

**CAP-C** bietet Vertrauenswürdigkeit durch die Analyse einer vollständigen Sicherheitsvorgabe für den zusammengesetzten TOE. Die SFRs in der ST des zusammengesetzten TOEs werden unter Verwendung der Evaluierungsergebnisse der Komponenten-TOEs (z. B. ST, Leitliniendokumentation), einer Spezifikation der Schnittstellen zwischen den Komponenten-TOEs und des TOE-Designs (mit Beschreibung der TSF-**Module**), das in den zusammengesetzten Entwicklungsinformationen enthalten ist, analysiert, um ein Verständnis für das Sicherheitsverhalten zu erlangen.

Die Analyse wird unterstützt durch unabhängige Prüfung der Schnittstellen der Basiskomponente, auf die sich die abhängige Komponente verlässt, entsprechend der Beschreibung in der Verlässlichkeitsinformation (nun auch einschließlich TOE-Design), durch den Nachweis der Entwicklerprüfung auf Grundlage der Verlässlichkeitsinformation, der Entwicklungsinformation und der Begründung der Zusammensetzung, sowie durch ausgewählte unabhängige Bestätigung der Prüfergebnisse des Entwicklers. Die Analyse wird außerdem von einer Anfälligkeitsanalyse des zusammengesetzten TOEs durch den Evaluator unterstützt, die den Nachweis der Widerstandsfähigkeit gegen Angreifer mit **erweiterten-grundlegendem** Angriffspotential erbringt.

Dieses CAP ist eine sinnvolle Zunahme der Vertrauenswürdigkeit im Vergleich zu **CAP-B** durch die Forderung nach **umfangreicherer Designbeschreibung und nach einem Nachweis der Widerstandsfähigkeit gegen ein höheres Angriffspotential**.

Tabelle 12 — CAP-C

| Vertrauenswürdigkeitsklasse         | Vertrauenswürdigkeitskomponenten                                      |
|-------------------------------------|-----------------------------------------------------------------------|
| ACO: Zusammensetzung                | ACO_COR.1 Begründung der Zusammensetzung                              |
|                                     | ACO_CTT.2 Strenge Schnittstellenprüfung                               |
|                                     | ACO_DEV.3 Detaillierter Nachweis des Designs                          |
|                                     | ACO_REL.2 Verlässlichkeitsinformation                                 |
|                                     | ACO_VUL.3 Erweitert-einfache Anfälligkeitsanalyse der Zusammensetzung |
| AGD: Leitliniendokumente            | AGD_OPE.1 Operative Leitlinien für Benutzer                           |
|                                     | AGD_PRE.1 Vorbereitende Verfahren                                     |
| ALC: Unterstützung des Lebenszyklus | ALC_CMC.1 Kennzeichnung des TOEs                                      |
|                                     | ALC_CMS.2 CM Abdeckung für Teile des TOEs                             |

| Vertrauenswürdigkeitsklasse             | Vertrauenswürdigkeitskomponenten                  |
|-----------------------------------------|---------------------------------------------------|
| ASE: Evaluierung der Sicherheitsvorgabe | ASE_CCL.1 Konformitätsansprüche                   |
|                                         | ASE_ECD.1 Erweiterte Komponentendefinition        |
|                                         | ASE_INT.1 ST Einleitung                           |
|                                         | ASE_OBJ.2 Sicherheitszielsetzungen                |
|                                         | ASE_REQ.2 Abgeleitete Sicherheitsanforderungen    |
|                                         | ASE_SPD.1 Sicherheitsproblemdefinition            |
|                                         | ASE_TSS.1 Zusammenfassende Spezifikation des TOEs |

## 9 Klasse APE: Evaluierung des Schutzprofils

Evaluierung eines PP ist erforderlich zum Nachweis, dass ein PP sachgerecht und in sich konsistent ist und, wenn das PP auf einem oder mehreren anderen PP's oder Paketen basiert, dass das PP eine korrekte Instanziierung dieser PP's und Pakete darstellt. Diese Eigenschaften sind erforderlich, damit das PP für die Verwendung als Grundlage zum Schreiben einer ST oder anderer PP's geeignet ist.

Dieser Abschnitt sollte in Verbindung mit Anhang A, Anhang B und Anhang C von ISO/IEC 15408-1:2009 verwendet werden, da diese Anhänge die hier dargestellten Konzepte verdeutlichen und eine Vielzahl an Beispielen zeigen.

Diese Norm definiert die folgenden zwei Sicherheitspakete für die Evaluierung von PP's:

- a) PP-Evaluierungspaket mit niedriger Vertrauenswürdigkeit;
- b) (Standard-) PP-Evaluierungspaket.

Die Vertrauenswürdigkeitskomponenten für diese Pakete sind in Tabelle 13 definiert.

**Tabelle 13 — PP-Sicherheitspakete**

| Vertrauenswürdigkeitsklasse   | Vertrauenswürdigkeitsfamilie | Vertrauenswürdigkeitskomponente       |    |
|-------------------------------|------------------------------|---------------------------------------|----|
|                               |                              | PP mit niedriger Vertrauenswürdigkeit | PP |
| Evaluierung des Schutzprofils | APE_CCL                      | 1                                     | 1  |
|                               | APE_ECD                      | 1                                     | 1  |
|                               | APE_INT                      | 1                                     | 1  |
|                               | APE_OBJ                      | 1                                     | 2  |
|                               | APE_REQ                      | 1                                     | 2  |
|                               | APE_SPD                      |                                       | 1  |

Bild 8 zeigt die Familien in dieser Klasse sowie die Hierarchie der Komponenten innerhalb der Familien.

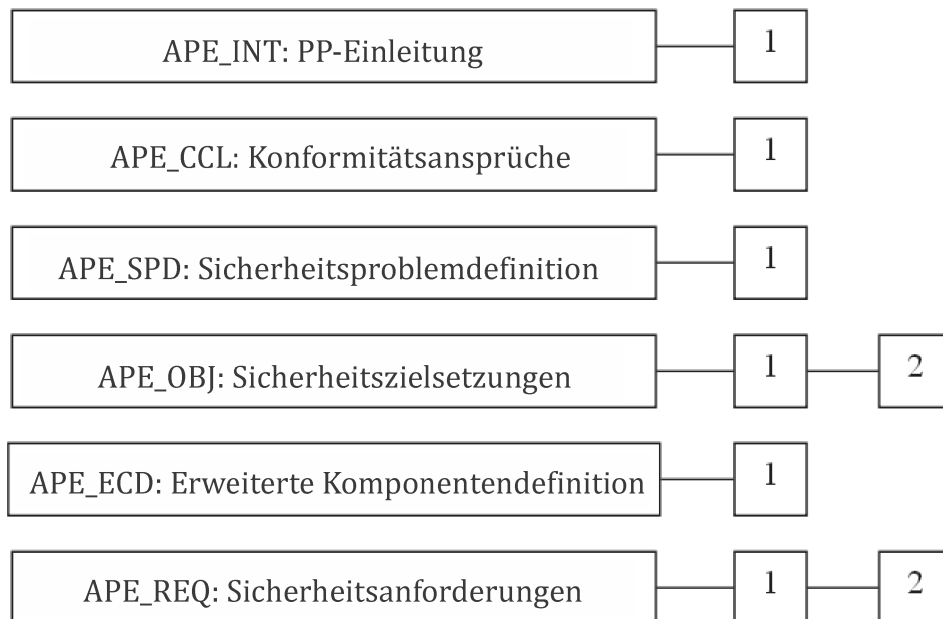


**Bild 8 — APE: Evaluierung des Schutzprofils, Klassenaufbau**

## 9.1 PP-Einleitung (APE\_INT)

### 9.1.1 Ziele

Das Ziel dieser Familie ist die ausformulierte Beschreibung des TOEs.

Evaluierung der PP-Einleitung ist erforderlich, um nachzuweisen, dass das PP korrekt identifiziert wurde und dass die PP-Verweisung und der TOE-Überblick konsistent miteinander sind.

### 9.1.2 APE\_INT.1 PP-Einleitung

Abhängigkeiten: keine Abhängigkeiten.

#### 9.1.2.1 Entwickleraktionselemente

##### 9.1.2.1.1 APE\_INT.1.1D

**Der Entwickler muss eine PP-Einleitung bereitstellen.**

#### 9.1.2.2 Elemente von Inhalt und Darstellung

##### 9.1.2.2.1 APE\_INT.1.1C

**Die PP-Einleitung muss eine PP-Verweisung und einen TOE-Überblick enthalten.**

##### 9.1.2.2.2 APE\_INT.1.2C

**Die PP-Verweisung muss das PP eindeutig identifizieren.**

#### 9.1.2.2.3 APE\_INT.1.3C

Der TOE-Überblick muss die Verwendung und wesentliche Sicherheitsmerkmale des TOEs zusammenfassen.

#### 9.1.2.2.4 APE\_INT.1.4C

Der TOE-Überblick muss den TOE-Typ identifizieren.

#### 9.1.2.2.5 APE\_INT.1.5C

Der TOE-Überblick muss jede nicht im TOE enthaltene, aber für den TOE verfügbare Hardware/Software/Firmware identifizieren.

### 9.1.2.3 Evaluatorenaktionselemente

#### 9.1.2.3.1 APE\_INT.1.1E

Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

## 9.2 Konformitätsansprüche (APE\_CCL)

### 9.2.1 Ziele

Das Ziel dieser Familie ist die Bestimmung der Gültigkeit des Konformitätsanspruchs. Zusätzlich spezifiziert diese Familie, wie STs und andere PPs Konformität mit dem PP beanspruchen müssen.

### 9.2.2 APE\_CCL.1 Konformitätsansprüche

Abhängigkeiten: APE\_INT.1 PP Einleitung

APE\_ECD.1 Erweiterte Komponentendefinition

APE\_REQ.1 Festgelegte Sicherheitsanforderungen

#### 9.2.2.1 Entwickleraktionselemente

##### 9.2.2.1.1 APE\_CCL.1.1D

Der Entwickler muss einen Konformitätsanspruch bereitstellen.

##### 9.2.2.1.2 APE\_CCL.1.2D

Der Entwickler muss eine Begründung zum Konformitätsanspruch bereitstellen.

##### 9.2.2.1.3 APE\_CCL.1.3D

Der Entwickler muss eine Konformitätserklärung bereitstellen.

#### 9.2.2.2 Elemente von Inhalt und Darstellung

##### 9.2.2.2.1 APE\_CCL.1.1C

Der Konformitätsanspruch muss einen Konformitätsanspruch nach ISO/IEC 15408 enthalten, der die Version von ISO/IEC 15408 angibt, mit der das PP Konformität beansprucht.

#### 9.2.2.2.2 APE\_CCL.1.2C

Der Konformitätsanspruch nach ISO/IEC 15408 muss die Konformität des PP mit ISO/IEC 15408-2 entweder als ISO/IEC 15408-2-konform oder ISO/IEC 15408-2-erweitert beschreiben.

#### 9.2.2.2.3 APE\_CCL.1.3C

Der Konformitätsanspruch nach ISO/IEC 15408 muss die Konformität des PP mit ISO/IEC 15408-3 entweder als ISO/IEC 15408-3-konform oder ISO/IEC 15408-3-erweitert beschreiben.

#### 9.2.2.2.4 APE\_CCL.1.4C

Der Konformitätsanspruch nach ISO/IEC 15408 muss mit der erweiterten Komponentendefinition konsistent sein.

#### 9.2.2.2.5 APE\_CCL.1.5C

Der Konformitätsanspruch muss alle PPs und Sicherheitsanforderungspakete identifizieren, mit denen das PP Konformität beansprucht.

#### 9.2.2.2.6 APE\_CCL.1.6C

Der Konformitätsanspruch muss jede Konformität des PP mit einem Paket entweder als Paket-konform oder Paket-ergänzt beschreiben.

#### 9.2.2.2.7 APE\_CCL.1.7C

Die Begründung für den Konformitätsanspruch muss nachweisen, dass der TOE-Typ mit dem TOE-Typ in den PPs konsistent ist, für die Konformität beansprucht wird.

#### 9.2.2.2.8 APE\_CCL.1.8C

Die Begründung für den Konformitätsanspruch muss nachweisen, dass die Aussage zur Sicherheitsproblemdefinition mit der Aussage zur Sicherheitsproblemdefinition in den PPs konsistent ist, für die Konformität beansprucht wird.

#### 9.2.2.2.9 APE\_CCL.1.9C

Die Begründung für den Konformitätsanspruch muss nachweisen, dass die Aussage zu den Sicherheitszielsetzungen mit der Aussage zu den Sicherheitszielsetzungen in den PPs konsistent ist, für die Konformität beansprucht wird.

#### 9.2.2.2.10 APE\_CCL.1.10C

Die Begründung für den Konformitätsanspruch muss nachweisen, dass die Aussage zu den Sicherheitsanforderungen mit der Aussage zu den Sicherheitsanforderungen in den PPs konsistent ist, für die Konformität beansprucht wird.

#### 9.2.2.2.11 APE\_CCL.1.11C

Die Konformitätserklärung muss die geforderte Konformität aller PPs/STs mit dem PP als strikte PP-Konformität oder nachweisliche PP-Konformität beschreiben.

### 9.2.2.3 Evaluatorenaktionselemente

#### 9.2.2.3.1 APE\_CCL.1.1E

**Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.**

## 9.3 Sicherheitsproblemdefinition (APE\_SPD)

### 9.3.1 Ziele

Dieser Teil des PPs definiert das vom TOE zu behandelnde Sicherheitsproblem und die Betriebsumgebung des TOEs.

Evaluierung der Sicherheitsproblemdefinition ist erforderlich, um nachzuweisen, dass das vom TOE zu behandelnde Sicherheitsproblem und seine Betriebsumgebung klar definiert sind.

### 9.3.2 APE\_SPD.1 Sicherheitsproblemdefinition

Abhängigkeiten: keine Abhängigkeiten.

#### 9.3.2.1 Entwickleraktionselemente

##### 9.3.2.1.1 APE\_SPD.1.1D

**Der Entwickler muss eine Sicherheitsproblemdefinition bereitstellen.**

#### 9.3.2.2 Elemente von Inhalt und Darstellung

##### 9.3.2.2.1 APE\_SPD.1.1C

**Die Sicherheitsproblemdefinition muss die Bedrohungen beschreiben.**

##### 9.3.2.2.2 APE\_SPD.1.2C

**Alle Bedrohungen müssen in Bezug auf einen Bedrohungsagenten, einen Vermögenswert und eine unerwünschte Aktion beschrieben werden.**

##### 9.3.2.2.3 APE\_SPD.1.3C

**Die Sicherheitsproblemdefinition muss die OSPs beschreiben.**

##### 9.3.2.2.4 APE\_SPD.1.4C

**Die Sicherheitsproblemdefinition muss die Annahmen über die Betriebsumgebung des TOE beschreiben.**

### 9.3.2.3 Evaluatorenaktionselemente

#### 9.3.2.3.1 APE\_SPD.1.1E

**Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.**

## 9.4 Sicherheitszielsetzungen (APE\_OBJ)

### 9.4.1 Ziele

Die Sicherheitszielsetzungen sind eine präzise Aussage zur angestrebten Antwort auf das Sicherheitsproblem, das durch die Familie „Sicherheitsproblemdefinition“ (APE\_SPD) definiert ist.

Evaluierung der Sicherheitszielsetzungen ist erforderlich, um nachzuweisen, dass die Sicherheitszielsetzungen die Sicherheitsproblemdefinition angemessen und vollständig behandeln und dass die Aufteilung dieses Problems zwischen dem TOE seiner Betriebsumgebung klar definiert ist.

### 9.4.2 Komponentenebenen

Die Komponenten in dieser Familie sind danach eingestuft, ob sie nur Sicherheitszielsetzungen für die Betriebsumgebung oder auch Sicherheitszielsetzungen für den TOE vorschreiben.

### 9.4.3 APE\_OBJ.1 Sicherheitszielsetzungen für die Betriebsumgebung

Abhängigkeiten: keine Abhängigkeiten.

#### 9.4.3.1 Entwickleraktionselemente

##### 9.4.3.1.1 APE\_OBJ.1.1D

**Der Entwickler muss eine Aussage zu Sicherheitszielsetzungen bereitstellen.**

#### 9.4.3.2 Elemente von Inhalt und Darstellung

##### 9.4.3.2.1 APE\_OBJ.1.1C

**Die Aussage zu den Sicherheitszielsetzungen muss die Sicherheitszielsetzungen für die Betriebsumgebung beschreiben.**

#### 9.4.3.3 Evaluatorenaktionselemente

##### 9.4.3.3.1 APE\_OBJ.1.1E

**Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.**

### 9.4.4 APE\_OBJ.2 Sicherheitszielsetzungen

Abhängigkeiten: APE\_SPD.1 Sicherheitsproblemdefinition

#### 9.4.4.1 Entwickleraktionselemente

##### 9.4.4.1.1 APE\_OBJ.2.1D

**Der Entwickler muss eine Aussage zu Sicherheitszielsetzungen bereitstellen.**

##### 9.4.4.1.2 APE\_OBJ.2.2D

**Der Entwickler muss eine Begründung für die Sicherheitszielsetzungen bereitstellen.**

#### 9.4.4.2 Elemente von Inhalt und Darstellung

##### 9.4.4.2.1 APE\_OBJ.2.1C

Die Aussage zu Sicherheitszielsetzungen muss die Sicherheitszielsetzungen für den **TOE und die Sicherheitszielsetzungen für die** Betriebsumgebung beschreiben.

##### 9.4.4.2.2 APE\_OBJ.2.2C

Die Begründung für die Sicherheitszielsetzungen muss jede Sicherheitszielsetzung für den TOE zurückführen zu den Bedrohungen, die durch diese Sicherheitszielsetzung abgewehrt werden und zu den OSPs, die durch diese Sicherheitszielsetzung durchgesetzt werden.

##### 9.4.4.2.3 APE\_OBJ.2.3C

Die Begründung für die Sicherheitszielsetzungen muss jede Sicherheitszielsetzung für die Betriebsumgebung zurückführen zu den Bedrohungen, die durch diese Sicherheitszielsetzung abgewehrt werden, zu den OSPs, die durch diese Sicherheitszielsetzung durchgesetzt werden, und zu den Annahmen, die durch diese Sicherheitszielsetzung eingehalten werden.

##### 9.4.4.2.4 APE\_OBJ.2.4C

Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen alle Bedrohungen abwehren.

##### 9.4.4.2.5 APE\_OBJ.2.5C

Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen alle OSPs durchsetzen.

##### 9.4.4.2.6 APE\_OBJ.2.6C

Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen für die Betriebsumgebung alle Annahmen einhalten.

#### 9.4.4.3 Evaluatorenaktionselemente

##### 9.4.4.3.1 APE\_OBJ.2.1E

Der Evaluator muss bestätigen, dass die bereitgestellten Informationen alle Anforderungen an Inhalt und Darstellung des Nachweises erfüllen.

### 9.5 Erweiterte Komponentendefinition (APE\_ECD)

#### 9.5.1 Ziele

Erweiterte Sicherheitsanforderungen sind Anforderungen, die nicht auf Komponenten aus ISO/IEC 15408-2 oder diesem Teil von ISO/IEC 15408 basieren, sondern auf vom PP-Autor definierten erweiterten Komponenten.

Evaluierung der Definition von erweiterten Komponenten ist erforderlich zur Bestimmung, dass sie klar und eindeutig sind und dass sie erforderlich sind, d. h. sie können unter Verwendung bestehender Komponenten von ISO/IEC 15408-2 oder Komponenten dieses Teils von ISO/IEC 15408 nicht klar formuliert werden.