

**DIN EN ISO/IEC 15408-1**

ICS 35.030

Ersatz für  
die 2011-03 zurückgezogene  
Norm  
DIN ISO/IEC 15408-1:2007-11

**Informationstechnik –  
IT-Sicherheitsverfahren –  
Evaluationskriterien für IT-Sicherheit –  
Teil 1: Einführung und allgemeines Modell (ISO/IEC 15408-1:2009);  
Deutsche Fassung EN ISO/IEC 15408-1:2020**

Information technology –  
Security techniques –  
Evaluation criteria for IT security –  
Part 1: Introduction and general model (ISO/IEC 15408-1:2009);  
German version EN ISO/IEC 15408-1:2020

Technologies de l'information –  
Techniques de sécurité –  
Critères d'évaluation pour la sécurité TI –  
Partie 1: Introduction et modèle général (ISO/IEC 15408-1:2009);  
Version allemande EN ISO/IEC 15408-1:2020

Gesamtumfang 84 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

## **Nationales Vorwort**

Der Text von ISO/IEC 15408-1:2009 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 15408-1:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Gremium 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 15408-2 | siehe | DIN EN ISO/IEC 15408-2 (z. Z. Entwurf) |
| ISO/IEC 15408-3 | siehe | DIN EN ISO/IEC 15408-3 (z. Z. Entwurf) |
| ISO/IEC 18045   | siehe | DIN EN ISO/IEC 18045 (z. Z. Entwurf)   |
| ISO/IEC 19790   | siehe | DIN EN ISO/IEC 19790                   |
| ISO/IEC 27001   | siehe | DIN EN ISO/IEC 27001                   |
| ISO/IEC 27002   | siehe | DIN EN ISO/IEC 27002                   |

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 15408-1:2007-11 wurden folgende Änderungen vorgenommen:

- a) Abschnitt 3: Korrektur der Begriffe „Sicherheitsproblem“ und „Sicherheitsdomänen“;
- b) Abschnitt 8.3: Erklärung der strikten Konformität, Streichung des früheren Bildes 4;
- c) Dokument redaktionell überarbeitet.

## **Frühere Ausgaben**

DIN ISO/IEC 15408-1: 2001-03, 2007-11

## Nationaler Anhang NA (informativ)

### Literaturhinweise

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

DIN EN ISO/IEC 15408-3, *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 3: Komponenten zur Sicherheitskontrolle*

DIN EN ISO/IEC 18045, *Informationstechnik — Sicherheitstechniken — Methodik für die Bewertung der IT-Sicherheit*

DIN EN ISO/IEC 19790, *Informationstechnik — Sicherheitstechniken — Sicherheitsanforderungen für kryptografische Module*

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen*

DIN EN ISO/IEC 27002, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen*

— Leerseite —

Deutsche Fassung

Informationstechnik —  
IT-Sicherheitsverfahren —  
Evaluationskriterien für IT-Sicherheit —  
Teil 1: Einführung und allgemeines Modell  
(ISO/IEC 15408-1:2009)

Information technology —  
Security techniques —  
Evaluation criteria for IT security —  
Part 1: Introduction and general model  
(ISO/IEC 15408-1:2009)

Technologies de l'information —  
Techniques de sécurité —  
Critères d'évaluation pour la sécurité TI —  
Partie 1: Introduction et modèle général  
(ISO/IEC 15408-1:2009)

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 und elektrotechnischen Komitees 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 Centre:  
Rue de la Science 23, B-1040 Brussels

## Inhalt

|                                                       | Seite |
|-------------------------------------------------------|-------|
| Europäisches Vorwort .....                            | 5     |
| Vorwort .....                                         | 6     |
| Einleitung .....                                      | 7     |
| 1 Anwendungsbereich .....                             | 9     |
| 2 Normative Verweisungen .....                        | 9     |
| 3 Begriffe .....                                      | 9     |
| 3.1 In ISO/IEC 15408 verwendete Begriffe .....        | 9     |
| 3.2 Begriffe in Zusammenhang mit der Klasse ADV ..... | 18    |
| 3.3 Begriffe in Zusammenhang mit der Klasse AGD ..... | 22    |
| 3.4 Begriffe in Zusammenhang mit der Klasse ALC ..... | 23    |
| 3.5 Begriffe in Zusammenhang mit der Klasse AVA ..... | 27    |
| 3.6 Begriffe in Zusammenhang mit der Klasse ACO ..... | 27    |
| 4 Symbole und Abkürzungen .....                       | 28    |
| 5 Übersicht .....                                     | 29    |
| 5.1 Allgemein .....                                   | 29    |
| 5.2 Der Evaluierungsgegenstand (TOE) .....            | 29    |
| 5.2.1 Unterschiedliche Darstellungen des TOEs .....   | 30    |
| 5.2.2 Unterschiedliche Konfigurationen des TOEs ..... | 30    |
| 5.3 Zielgruppe von ISO/IEC 15408 .....                | 31    |
| 5.3.1 Verbraucher .....                               | 31    |
| 5.3.2 Entwickler .....                                | 31    |
| 5.3.3 Evaluatoren .....                               | 31    |
| 5.3.4 Weitere .....                                   | 31    |
| 5.4 Die verschiedenen Teile von ISO/IEC 15408 .....   | 32    |
| 5.5 Evaluierungskontext .....                         | 33    |
| 6 Allgemeines Modell .....                            | 33    |
| 6.1 Einführung in das allgemeine Modell .....         | 33    |
| 6.2 Vermögenswerte und Gegenmaßnahmen .....           | 33    |
| 6.2.1 Angemessenheit der Gegenmaßnahmen .....         | 36    |
| 6.2.2 Korrektheit des TOEs .....                      | 37    |
| 6.2.3 Korrektheit der Betriebsumgebung .....          | 37    |
| 6.3 Evaluierung .....                                 | 38    |
| 7 Anpassung von Sicherheitsanforderungen .....        | 39    |
| 7.1 Operationen .....                                 | 39    |
| 7.1.1 Die Operation Iteration .....                   | 39    |
| 7.1.2 Die Operation Zuweisung .....                   | 40    |
| 7.1.3 Die Operation Auswahl .....                     | 40    |
| 7.1.4 Die Operation Präzisierung .....                | 41    |
| 7.2 Abhängigkeiten zwischen Komponenten .....         | 41    |
| 7.3 Erweiterte Komponenten .....                      | 42    |
| 8 Schutzprofile und Pakete .....                      | 42    |
| 8.1 Einleitung .....                                  | 42    |
| 8.2 Pakete .....                                      | 42    |

|                                                                          |                                                                                    |           |
|--------------------------------------------------------------------------|------------------------------------------------------------------------------------|-----------|
| 8.3                                                                      | Schutzprofile .....                                                                | 43        |
| 8.4                                                                      | Verwendung von PPs und Paketen .....                                               | 45        |
| 8.5                                                                      | Verwendung mehrerer Schutzprofile .....                                            | 46        |
| 9                                                                        | Evaluierungsergebnisse .....                                                       | 46        |
| 9.1                                                                      | Einleitung .....                                                                   | 46        |
| 9.2                                                                      | Ergebnisse einer PP-Evaluierung .....                                              | 47        |
| 9.3                                                                      | Ergebnisse einer ST-/TOE-Evaluierung .....                                         | 47        |
| 9.4                                                                      | Konformitätsanspruch .....                                                         | 47        |
| 9.5                                                                      | Verwendung der ST-/TOE-Evaluierungsergebnisse .....                                | 48        |
| <b>Anhang A (informativ) Spezifikation von Sicherheitsvorgaben .....</b> |                                                                                    | <b>50</b> |
| A.1                                                                      | Ziel und Aufbau dieses Anhangs .....                                               | 50        |
| A.2                                                                      | Verpflichtender Inhalt einer ST .....                                              | 50        |
| A.3                                                                      | Verwendung einer ST .....                                                          | 51        |
| A.3.1                                                                    | Wie eine ST verwendet werden sollte .....                                          | 51        |
| A.3.2                                                                    | Wie eine ST nicht verwendet werden sollte .....                                    | 52        |
| A.4                                                                      | ST-Einleitung (ASE_INT) .....                                                      | 52        |
| A.4.1                                                                    | ST-Verweisung und TOE-Verweisung .....                                             | 52        |
| A.4.2                                                                    | TOE-Überblick .....                                                                | 53        |
| A.4.3                                                                    | TOE-Beschreibung .....                                                             | 54        |
| A.5                                                                      | Konformitätsansprüche (ASE_CCL) .....                                              | 55        |
| A.6                                                                      | Sicherheitsproblemdefinition (ASE_SPD) .....                                       | 55        |
| A.6.1                                                                    | Einleitung .....                                                                   | 55        |
| A.6.2                                                                    | Bedrohungen .....                                                                  | 56        |
| A.6.3                                                                    | Organisatorische Sicherheitsrichtlinie (OSP) .....                                 | 56        |
| A.6.4                                                                    | Annahmen .....                                                                     | 56        |
| A.7                                                                      | Sicherheitszielsetzungen (ASE_OBJ) .....                                           | 57        |
| A.7.1                                                                    | Allgemeine Lösung .....                                                            | 57        |
| A.7.2                                                                    | Teillösungen .....                                                                 | 58        |
| A.7.3                                                                    | Beziehung zwischen Sicherheitszielsetzungen und Sicherheitsproblemdefinition ..... | 59        |
| A.7.4                                                                    | Sicherheitszielsetzungen: Schlussfolgerung .....                                   | 60        |
| A.8                                                                      | Erweiterte Komponentendefinition (ASE_ECD) .....                                   | 60        |
| A.9                                                                      | Sicherheitsanforderungen (ASE_REQ) .....                                           | 61        |
| A.9.1                                                                    | Sicherheitsfunktionsanforderungen (SFRs) .....                                     | 61        |
| A.9.2                                                                    | Vertrauenswürdigkeitsanforderungen (SARs) .....                                    | 62        |
| A.9.3                                                                    | SARs und die Begründung der Sicherheitsanforderungen .....                         | 63        |
| A.9.4                                                                    | Sicherheitsanforderungen: Schlussfolgerung .....                                   | 63        |
| A.10                                                                     | Zusammenfassende Spezifikation des TOEs (ASE_TSS) .....                            | 64        |
| A.11                                                                     | Fragen, die mit einer ST beantwortet werden können .....                           | 64        |
| A.12                                                                     | Sicherheitsvorgaben mit niedriger Vertrauenswürdigkeit .....                       | 65        |
| A.13                                                                     | Verweisen auf andere Normen in einer ST .....                                      | 66        |
| <b>Anhang B (informativ) Spezifikation von Schutzprofilen .....</b>      |                                                                                    | <b>68</b> |
| B.1                                                                      | Ziel und Aufbau dieses Anhangs .....                                               | 68        |
| B.2                                                                      | Verpflichtender Inhalt eines PPs .....                                             | 68        |
| B.3                                                                      | Verwendung eines PPs .....                                                         | 69        |
| B.3.1                                                                    | Wie ein PP verwendet werden sollte .....                                           | 69        |
| B.3.2                                                                    | Wie ein PP nicht verwendet werden sollte .....                                     | 70        |
| B.4                                                                      | PP-Einleitung (APE_INT) .....                                                      | 70        |
| B.4.1                                                                    | PP-Verweisung .....                                                                | 70        |
| B.4.2                                                                    | TOE-Überblick .....                                                                | 70        |
| B.5                                                                      | Konformitätsansprüche (APE_CCL) .....                                              | 71        |
| B.6                                                                      | Sicherheitsproblemdefinition (APE_SPD) .....                                       | 72        |
| B.7                                                                      | Sicherheitszielsetzungen (APE_OBJ) .....                                           | 72        |
| B.8                                                                      | Erweiterte Komponentendefinition (APE_ECD) .....                                   | 72        |
| B.9                                                                      | Sicherheitsanforderungen (APE_REQ) .....                                           | 72        |

|                                                       |                                                       |    |
|-------------------------------------------------------|-------------------------------------------------------|----|
| B.10                                                  | Zusammenfassende Spezifikation des TOEs.....          | 72 |
| B.11                                                  | Schutzprofile mit niedriger Vertrauenswürdigkeit..... | 72 |
| B.12                                                  | Verweisen auf andere Normen in einem PP .....         | 73 |
| Anhang C (informativ) Leitlinien für Operationen..... |                                                       | 74 |
| C.1                                                   | Einleitung .....                                      | 74 |
| C.2                                                   | Beispiele für Operationen .....                       | 74 |
| C.2.1                                                 | Die Operation Iteration .....                         | 74 |
| C.2.2                                                 | Die Operation Zuweisung .....                         | 74 |
| C.2.3                                                 | Die Operation Auswahl.....                            | 74 |
| C.2.4                                                 | Die Operation Präzisierung .....                      | 75 |
| C.3                                                   | Organisation von Komponenten .....                    | 75 |
| C.3.1                                                 | Klasse .....                                          | 76 |
| C.3.2                                                 | Familie .....                                         | 76 |
| C.3.3                                                 | Komponente .....                                      | 76 |
| C.3.4                                                 | Element.....                                          | 76 |
| C.4                                                   | Erweiterte Komponenten .....                          | 76 |
| C.4.1                                                 | Wie erweiterte Komponenten definiert werden .....     | 76 |
| Anhang D (informativ) PP-Konformität .....            |                                                       | 78 |
| D.1                                                   | Einleitung .....                                      | 78 |
| D.2                                                   | Strikte Konformität.....                              | 78 |
| D.3                                                   | Nachweisliche Konformität .....                       | 79 |
| Literaturhinweise.....                                |                                                       | 80 |

## **Europäisches Vorwort**

Der Text von ISO/IEC 15408-1:2009 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 15408-1:2020 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 15408-1:2009 wurde von CEN als EN ISO/IEC 15408-1:2020 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. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Internationale Normen werden in Übereinstimmung mit den Gestaltungsregeln von 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 ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

ISO/IEC 15408-1 wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques*, 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 findet sich unter <http://www.commoncriteriaportal.org/cc/>

Diese dritte Fassung ersetzt die zweite Fassung (ISO/IEC 15408-1:2005), die technisch überarbeitet wurde.

ISO/IEC 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 15408-1:2009 enthält die folgenden, allgemeinen redaktionellen Korrekturen:

- Terminologie: Korrekturen für die Begriffe „Sicherheitsproblem“ und „Sicherheitsdomäne(n)“;
- 8.3: Erklärung der strikten Konformität, Entfernung von vorherigem Bild 4.

## Einleitung

ISO/IEC 15408 ermöglicht die Vergleichbarkeit von Ergebnissen unabhängiger Sicherheitsevaluierungen. ISO/IEC 15408 erreicht dies durch eine einheitliche Reihe von Anforderungen an die Sicherheitsfunktionalität von IT-Produkten und an Maßnahmen zur Zusicherung der Vertrauenswürdigkeit, die auf diese IT-Produkte während einer Sicherheitsevaluierung angewendet werden. Diese IT-Produkte können in Hardware, Firmware oder Software implementiert werden.

Durch den Evaluierungsprozess wird ein Vertrauensniveau hergestellt, dass die Sicherheitsfunktionalität dieser IT-Produkte und die auf diese IT-Produkte angewendeten Maßnahmen zur Zusicherung der Vertrauenswürdigkeit diese Anforderungen erfüllen. Die Evaluierungsergebnisse können die Verbraucher bei der Bestimmung unterstützen, ob diese IT-Produkte ihre Sicherheitsbedürfnisse erfüllen.

ISO/IEC 15408 ist hilfreich als Leitfaden für Entwicklung, Evaluierung und/oder Beschaffung von IT-Produkten mit Sicherheitsfunktionalität.

ISO/IEC 15408 ist absichtlich flexibel gestaltet, um einen großen Bereich an Evaluierungsmethoden für einen großen Bereich an Sicherheitseigenschaften einer Vielzahl von IT-Produkten abzudecken. Anwender dieser Norm werden daher darauf hingewiesen, sorgfältig vorzugehen, damit diese Flexibilität nicht zweckentfremdet wird. Wird ISO/IEC 15408 beispielsweise in Verbindung mit ungeeigneten Evaluierungsmethoden, irrelevanten Sicherheitseigenschaften oder unangemessenen IT-Produkten verwendet, kann dies zu bedeutungslosen Evaluierungsergebnissen führen.

Somit hat die Evaluierung eines IT-Produkts nur eine Bedeutung im Zusammenhang mit den beurteilten Sicherheitseigenschaften und den angewendeten Evaluierungsmethoden. Evaluierungsstellen wird empfohlen, Produkte, Eigenschaften und Methoden zur Bestimmung, ob eine Evaluierung bedeutungsvolle Ergebnisse liefern wird, sorgfältig zu prüfen. Zusätzlich wird Käufern evaluierter Produkte empfohlen, sorgfältig zu prüfen, ob das evaluierte Produkt in diesem Zusammenhang und für die bestimmte Situation und ihre Bedürfnisse nützlich und anwendbar ist.

ISO/IEC 15408 behandelt den Schutz von Vermögenswerten vor unautorisierter Offenlegung, Änderung oder Nutzungsausfall. Die Schutzkategorien für diese drei Ausfalltypen der Sicherheit werden allgemein Vertraulichkeit, Integrität und Verfügbarkeit genannt. ISO/IEC 15408 kann auch anwendbar sein auf Bereiche der IT-Sicherheit, die über diese drei Kategorien hinausgehen. ISO/IEC 15408 ist anwendbar auf von Menschen ausgelöste Risiken (böswillig oder anders geartet) und auf nicht von Menschen ausgelöste Risiken. ISO/IEC 15408 darf neben der IT-Sicherheit auch auf andere Bereiche der IT angewendet werden, aber die Norm erhebt für jene anderen Bereiche keinen Anspruch auf Anwendbarkeit.

Bestimmte Themen liegen außerhalb des Anwendungsbereichs von ISO/IEC 15408, weil sie besondere Techniken umfassen oder nur am Rande Teil der IT-Sicherheit sind. Einige dieser Themen sind unten aufgeführt.

- a) ISO/IEC 15408 umfasst keine Sicherheitsevaluierungskriterien zu administrativen Sicherheitsmaßnahmen, die sich nicht direkt auf die IT-Sicherheitsfunktionalität beziehen. Allerdings ist es eine anerkannte Tatsache, dass eine beträchtliche Erhöhung der Sicherheit oftmals durch administrative Maßnahmen im organisatorischen, personellen, physischen oder verfahrenstechnischem Bereich erreicht werden kann oder dadurch unterstützt wird.
- b) Auf die Evaluierung einiger technisch-physikalischer Aspekte der IT-Sicherheit wie elektromagnetische Emanationssteuerung wird nicht im Speziellen eingegangen, obwohl eine Vielzahl der behandelten Konzepte auf dieses Gebiet anwendbar sind.

- c) ISO/IEC 15408 behandelt nicht die Evaluierungsmethodologie, mit der die Kriterien angewendet werden sollten. Diese Methodologie ist in ISO/IEC 18045 enthalten.
- d) ISO/IEC 15408 behandelt nicht das administrative und rechtliche Rahmenwerk, mit dem die Kriterien von Evaluierungsinstanzen angewendet werden dürfen. Es wird jedoch erwartet, dass ISO/IEC 15408 für Evaluierungszwecke im Zusammenhang mit einem solchen Rahmenwerk verwendet wird.
- e) Die Verfahren zur Verwendung von Evaluierungsergebnissen in Akkreditierungen liegen außerhalb des Anwendungsbereichs von ISO/IEC 15408. Akkreditierung ist der administrative Prozess, bei dem die Berechtigung für den Betrieb eines IT-Produkts (oder einer Sammlung dergleichen) in seiner vollständigen Betriebsumgebung gewährt wird, einschließlich aller seiner Nicht-IT-Teile. Die Ergebnisse des Evaluierungsprozesses fließen in den Akkreditierungsprozess ein. Da allerdings andere Techniken für die Bewertung von Eigenschaften ohne Bezug zur IT und deren Beziehung zu Teilen der IT-Sicherheit besser geeignet sind, sollten Akkreditierer gesonderte Bestimmungen für diese Aspekte treffen.
- f) Die Kriterien für die Bewertung der charakteristischen Qualitäten von kryptographischen Algorithmen werden nicht in ISO/IEC 15408 behandelt. Sollte eine unabhängige Bewertung der mathematischen Eigenschaften der Kryptographie erforderlich sein, so muss der in ISO/IEC 15408 angewendete Evaluierungsplan solch eine Bewertung vorsehen.

Die im Dokument durchgängig verwendete ISO-Terminologie wie „kann“, „informativ“, „darf“, „normativ“, „muss“ und „sollte“ sind in den ISO-/IEC-Direktiven, Teil 2 festgelegt. Es ist zu beachten, dass der Begriff „sollte“ bei der Anwendung dieser Norm noch eine zusätzliche Bedeutung hat. Siehe Anmerkung unten. Die folgende Definition gilt für die Verwendung von „sollte“ in ISO/IEC 15408:

#### **sollte**

In normativen Texten zeigt „sollte“ an, „dass unter verschiedenen Möglichkeiten eine Möglichkeit als besonders zutreffend empfohlen wird, ohne andere zu erwähnen oder auszuschließen, oder dass eine bestimmte Vorgehensweise bevorzugt wird, aber nicht notwendigerweise erforderlich ist.“ (ISO/IEC-Direktiven, Teil 2).

**ANMERKUNG** ISO/IEC 15408 interpretiert „nicht notwendigerweise erforderlich“ so, dass die Wahl zugunsten einer anderen Möglichkeit eine Begründung zur Nichtverwendung der bevorzugten Option erfordert.

## 1 Anwendungsbereich

Dieser Teil von ISO/IEC 15408 legt die allgemeinen Konzepte und Prinzipien der IT-Sicherheitsbewertung fest und bestimmt das allgemeine Bewertungsmodell, das in verschiedenen Teilen der Norm verwendet wird, und das in seiner Gesamtheit als Grundlage für die Bewertung der Sicherheitseigenschaften von IT-Produkten vorgesehen ist.

Teil 1 bietet einen Überblick über alle Teile der Norm ISO/IEC 15408. Dieser Teil beschreibt die verschiedenen Teile der Norm, definiert die Begriffe und Abkürzungen zur Verwendung in allen Teilen der Norm, legt das Kernkonzept des Bewertungsgegenstands (TOE; en: target of evaluation) und den Bewertungszusammenhang fest und beschreibt die Zielgruppe, an die sich die Bewertungskriterien richten. Zu den für die Bewertung von IT-Produkten erforderlichen, grundlegenden Sicherheitskonzepten wird eine Einführung gegeben.

Teil 1 definiert die verschiedenen Operationen, mit denen die Funktionskomponenten und Vertrauenswürdigkeitskomponenten in ISO/IEC 15408-2 und ISO/IEC 15408-3 für die Verwendung der zulässigen Operationen angepasst werden dürfen.

Die grundlegenden Konzepte von Schutzprofilen (PP; en: protection profiles), Paketen von Sicherheitsanforderungen und das Thema Konformität werden spezifiziert und die Konsequenzen von Bewertung und Bewertungsergebnissen beschrieben. Dieser Teil von ISO/IEC 15408 enthält Leitlinien für die Spezifizierung von Sicherheitsvorgaben (ST; en: security targets) und beschreibt die Organisation von Bestandteilen im gesamten Modell. ISO/IEC 18045 enthält allgemeine Informationen über die Bewertungsmethodologie und bestimmt den Anwendungsbereich von Bewertungsplänen.

## 2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung von ISO/IEC 15408 Teil 1 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 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

## 3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

**ANMERKUNG** Dieser Abschnitt enthält nur diejenigen Begriffe, die innerhalb von ISO/IEC 15408 in spezieller Weise verwendet werden. Manche Kombinationen von in ISO/IEC 15408 verwendeten allgemeinen Begriffen sind daher nicht in diesem Abschnitt enthalten, werden aber der Klarheit wegen in dem Zusammenhang erläutert, in dem sie verwendet werden.

### 3.1 In ISO/IEC 15408 verwendete Begriffe

#### 3.1.1

##### **nachteilige Aktionen**

Aktionen, die von einem Bedrohungsagenten gegen ein Schutzobjekt durchgeführt werden

### 3.1.2

#### **Vermögenswert**

Entitäten, von denen anzunehmen ist, dass sie für den Eigentümer des TOEs einen Wert darstellen

### 3.1.3

#### **Zuweisung**

Spezifikation eines bezeichneten Parameters in einer Komponente (von ISO/IEC 15408) oder einer Anforderung

### 3.1.4

#### **Vertrauenswürdigkeit**

Vertrauensgrundlage, dass ein TOE die SFRs einhält

### 3.1.5

#### **Angriffspotential**

Maß für den erforderlichen Aufwand bei einem Angriff auf ein TOE, ausgedrückt in Form von Fachkenntnis, Ressourcen und Motivation des Angreifers

### 3.1.6

#### **Erweiterung**

Hinzufügen von einer oder mehreren Anforderung(en) zu einem Paket

### 3.1.7

#### **Authentisierungsdaten**

Informationen, die zur Überprüfung der angegebenen Identität eines Benutzers verwendet werden

### 3.1.8

#### **autorisierter Benutzer**

TOE-Benutzer, der in Übereinstimmung mit den SFRs eine Handlung durchführen darf

### 3.1.9

#### **Klasse**

eine Reihe von ISO/IEC 15408-Familien mit einem gemeinsamen Fokus

### 3.1.10

#### **kohärent**

logisch geordnet und mit einer erkennbaren Bedeutung

ANMERKUNG Im Zusammenhang mit Dokumentation bezieht sich dies sowohl auf den eigentlichen Text als auch auf die Struktur des Dokuments hinsichtlich der Verständlichkeit für die Zielgruppe.

### 3.1.11

#### **vollständig**

Eigenschaft, die angibt, dass alle erforderlichen Bestandteile einer Entität bereitgestellt wurden

ANMERKUNG In Bezug auf Dokumentation bedeutet dies, dass alle relevanten Informationen in der Dokumentation in einer solchen Detailliertheit beschrieben sind, dass auf der entsprechenden Abstraktionsebene keine weitere Erklärung erforderlich ist.

### 3.1.12

#### **Komponente**

kleinster selektierbarer Elementesatz, auf dem Anforderungen basieren können

### 3.1.13

#### **zusammengesetztes Vertrauenswürdigkeitspaket**

##### **CAP**

(en: Composed Assurance Package)

Vertrauenswürdigkeitspaket, bestehend aus Anforderungen, die auf ISO/IEC 15408-3 beruhen (vorwiegend auf der ACO-Klasse) und die einen Punkt der in ISO/IEC 15408 vorgegebenen zusammengesetzten Vertrauenswürdigkeitsskala repräsentieren

### 3.1.14

#### **bestätigen**

erklären, dass etwas detailliert und mit einer unabhängig bestimmten Angemessenheit geprüft wurde

ANMERKUNG Die erforderliche Stringenz hängt von der Art der betrachteten Einheit ab. Dieser Begriff wird nur für Evaluatorenaktionen verwendet.

### 3.1.15

#### **Konnektivität**

Eigenschaft des TOEs, die eine Interaktion mit IT-Entitäten außerhalb des TOEs ermöglicht

ANMERKUNG Dies schließt den Datenaustausch über verdrahtete oder drahtlose Verbindungen, über beliebige Entfernungen und in allen Umgebungen und Konfigurationen ein.

### 3.1.16

#### **widerspruchsfrei**

Beziehung zwischen zwei oder mehreren Entitäten, bei der keine offensichtlichen Widersprüche zwischen diesen Entitäten auftreten

### 3.1.17

#### **abwehren**, Verb

einem Angriff entgegenwirken, wobei die Auswirkung einer bestimmten Bedrohung abgemildert, aber nicht notwendigerweise ausgeremert wird

### 3.1.18

#### **nachweisliche Konformität**

Beziehung zwischen einer ST und einem PP, wobei die ST eine Lösung bereitstellt, welche das generische Sicherheitsproblem im PP löst

ANMERKUNG Das PP und die ST können völlig unterschiedliche Aussagen enthalten, die verschiedene Entitäten behandeln, verschiedene Konzepte verwenden usw. Die nachweisliche Konformität eignet sich auch für TOE-Typen, für die bereits mehrere ähnliche PPs existieren, so dass der ST-Autor auch die Konformität mit diesen PPs beanspruchen kann, um so Arbeit zu ersparen.

### 3.1.19

#### **demonstrieren**

Liefern einer Schlussfolgerung, die durch eine weniger strenge Analyse als einen „Beweis“ erlangt wurde

### 3.1.20

#### **Abhängigkeit**

Verhältnis zwischen Komponenten, bei dem gilt, dass wenn eine auf der abhängigen Komponente basierende Anforderung in einem PP, einer ST oder einem Paket enthalten ist, normalerweise auch eine Anforderung im PP, in der ST oder im Paket enthalten sein muss, die auf der Komponente basiert, von der die Abhängigkeit besteht

### 3.1.21

#### **beschreiben**

spezifische Einzelheiten zu einer Entität bereitstellen

### **3.1.22**

#### **bestimmen**

eine bestimmte Schlussfolgerung auf Basis einer unabhängigen Analyse bestätigen mit dem Ziel, eine bestimmte Schlussfolgerung zu erreichen

**ANMERKUNG** Die Verwendung dieses Begriffs setzt eine wirklich unabhängige Analyse voraus, in der Regel ohne dass eine vorhergehende Analyse durchgeführt wurde. Vergleiche die Begriffe „bestätigen“ oder „verifizieren“, welche voraussetzen, dass bereits eine Analyse durchgeführt wurde, welche überprüft werden muss.

### **3.1.23**

#### **Entwicklungsumgebung**

Umgebung, in der der TOE entwickelt wird

### **3.1.24**

#### **Element**

nicht unterteilbare Beschreibung einer Sicherheitsanforderung

### **3.1.25**

#### **sicherstellen**

eine starke kausale Abhängigkeit zwischen einer Aktion und deren Auswirkungen garantieren

**ANMERKUNG** Wenn diesem Begriff das Wort „helfen“ vorangestellt ist, weist dies darauf hin, dass die Auswirkung aufgrund nur dieser Aktion nicht sicher garantiert ist.

### **3.1.26**

#### **Evaluierung**

Bewertung eines PP, einer ST oder eines TOEs auf Grundlage definierter Kriterien

### **3.1.27**

#### **Vertrauenswürdigkeitsstufe**

##### **EAL-Stufe**

(en: Evaluation Assurance Level)

Reihe von aus ISO/IEC 15408-3 entnommenen Vertrauenswürdigkeitsanforderungen, die einem Punkt der in ISO/IEC 15408 definierten Vertrauenswürdigkeitsskala entsprechen, welche ein Sicherheitspaket bilden

### **3.1.28**

#### **Evaluierungsinstanz**

Institution, die für von Institutionen innerhalb einer bestimmten Gemeinschaft durchgeführte Evaluierungen die Anforderungen festlegt und die Qualität überwacht und die mittels eines Evaluierungsprogramms ISO/IEC 15408 für die jeweilige Gemeinschaft implementiert

### **3.1.29**

#### **Evaluierungsprogramm**

administratives und regulatorisches Rahmenwerk, auf dessen Basis ISO/IEC 15408 innerhalb einer bestimmten Gemeinschaft durch eine Evaluierungsinstanz umgesetzt wird

### **3.1.30**

#### **erschöpfend**

Merkmal eines methodischen Konzepts zur Durchführung einer Analyse oder Aktivität in Übereinstimmung mit einem eindeutigen Plan

**ANMERKUNG** Dieser Begriff wird in ISO/IEC 15408 bezüglich der Durchführung einer Analyse oder einer anderen Aktivität verwendet. Er ist mit „systematisch“ verwandt, ist aber erheblich stärker, da er nicht nur angibt, dass zur Durchführung der Analyse oder Aktivität ein methodischer Ansatz nach einem eindeutigen Plan befolgt wurde, sondern auch, dass der befolgte Plan ausreicht, um sicherzustellen, dass alle möglichen Verfahrensweisen durchgeführt wurden.

### **3.1.31**

#### **erklären**

ein Argument für die Begründung einer gewählten Vorgehensweise liefern

ANMERKUNG Dieser Begriff unterscheidet sich von den Begriffen „beschreiben“ und „demonstrieren“. Er soll die Frage nach dem „Warum“ beantworten, ohne Argumente dafür zu liefern, dass die gewählte Vorgehensweise notwendigerweise optimal war.

### **3.1.32**

#### **Erweiterung**

Hinzufügen von funktionellen Anforderungen, die nicht in ISO/IEC 15408-2 enthalten sind, zu einer ST oder eines PP und/oder Hinzufügen von Sicherheitsanforderungen, die nicht in ISO/IEC 15408-3 enthalten sind

### **3.1.33**

#### **externe Entität**

menschliche oder IT-Entität, die möglicherweise von außerhalb der TOE-Grenze mit dem TOE interagiert

ANMERKUNG Eine externe Entität kann auch als Benutzer bezeichnet werden.

### **3.1.34**

#### **Familie**

Satz von Komponenten, die eine ähnliche Zielsetzung haben, sich aber in Schwerpunkt oder Stringenz unterscheiden

### **3.1.35**

#### **formal**

ausgedrückt in einer Sprache mit begrenzter Syntax und definierter Semantik, basierend auf anerkannten mathematischen Konzepten

### **3.1.36**

#### **Leitliniendokumentation**

Dokumentation, die die Auslieferung, die Bereitstellung, den Betrieb, das Management und/oder die Verwendung des TOEs beschreibt

### **3.1.37**

#### **Identität**

Repräsentation, mit der Entitäten im Zusammenhang mit dem TOE eindeutig identifiziert werden (z. B. Benutzer, Prozesse oder Festplatten)

ANMERKUNG Ein Beispiel für eine solche Repräsentation ist eine Zeichenkette. Bei einem menschlichen Benutzer kann die Repräsentation der vollständige oder abgekürzte Name oder ein (nach wie vor eindeutiges) Pseudonym sein.

### **3.1.38**

#### **informal**

in der natürlichen Sprache ausgedrückt

### **3.1.39**

#### **Inter-TSF-Übertragung**

Datenkommunikation zwischen dem TOE und den Sicherheitsfunktionen anderer vertrauenswürdiger IT-Produkte

### **3.1.40**

#### **interner Kommunikationskanal**

Kommunikationskanal zwischen getrennten Teilen des TOEs

#### 3.1.41

##### **interne TOE-Übertragung**

Datenkommunikation zwischen getrennten Teilen des TOEs

#### 3.1.42

##### **in sich widerspruchsfrei**

es bestehen keine offensichtlichen Widersprüche zwischen irgendwelchen Aspekten einer Entität

ANMERKUNG In Bezug auf Dokumentation bedeutet dies, dass keine Aussagen in der Dokumentation enthalten sein können, die als widersprüchlich zueinander interpretiert werden können.

#### 3.1.43

##### **Iteration**

Verwendung der gleichen Komponente, um zwei oder mehr unterschiedliche Anforderungen auszudrücken

#### 3.1.44

##### **Begründung**

Analyse, die zu einer Schlussfolgerung führt

ANMERKUNG „Begründung“ ist stringenter als eine Demonstration. Dieser Begriff erfordert erhebliche Stringenz, indem jeder Schritt eines logischen Arguments sehr sorgfältig und gründlich erläutert wird.

#### 3.1.45

##### **Objekt**

passive Entität im TOE, die Informationen enthält oder empfängt und an der Subjekte Operationen durchführen

#### 3.1.46

##### **Operation**

<an einer Komponente von ISO/IEC 15408> Modifikation oder Wiederholung einer Komponente

ANMERKUNG Zulässige Operationen an Komponenten sind Zuweisung, Iteration, Präzisierung und Auswahl.

#### 3.1.47

##### **Operation**

<an einem Objekt> spezifische Aktion, die durch ein Subjekt an einem Objekt durchgeführt wird

#### 3.1.48

##### **Betriebsumgebung**

Umgebung, in der der TOE betrieben wird

#### 3.1.49

##### **organisatorische Sicherheitsrichtlinie**

##### **OSP**

(en: Organisational Security Policy)

Satz von Sicherheitsregeln, -verfahren oder -leitlinien für eine Organisation

ANMERKUNG Eine Richtlinie kann sich auf eine spezifische Betriebsumgebung beziehen.

#### 3.1.50

##### **Paket**

benannter Satz von Anforderungen bezüglich der Sicherheitsfunktionalität oder Vertrauenswürdigkeit

ANMERKUNG Ein Beispiel für ein Paket ist „EAL 3“.

### 3.1.51

#### **Schutzprofilevaluierung**

Bewertung eines PP auf Grundlage definierter Kriterien

### 3.1.52

#### **Schutzprofil**

##### **PP**

(en: Protection Profile)

implementierungsunabhängige Beschreibung der Sicherheitsanforderungen für einen TOE-Typ

### 3.1.53

#### **beweisen**

Übereinstimmung im mathematischen Sinn durch formale Analyse aufzeigen

ANMERKUNG Der Begriff ist in jeder Beziehung vollständig stringent. Im Allgemeinen wird „beweisen“ verwendet, wenn die Übereinstimmung zwischen zwei TSF-Darstellungen auf einem hohen Stringenzniveau dargestellt werden soll.

### 3.1.54

#### **Präzisierung**

Hinzufügen von Details zu einer Komponente

### 3.1.55

#### **Rolle**

vordefinierter Regelsatz, der die zulässigen Interaktionen zwischen einem Benutzer und dem TOE festlegt

### 3.1.56

#### **Geheimnis**

Informationen, die nur autorisierten Benutzern und/oder der TSF bekannt sein dürfen, um ein spezifisches SFP durchzusetzen

### 3.1.57

#### **sicherer Zustand**

Zustand, in dem die TSF-Daten konsistent sind und die TSF die ordnungsgemäße Durchsetzung der SFRs fortlaufend wahrnimmt

### 3.1.58

#### **Sicherheitsattribut**

Eigenschaft von Subjekten, Benutzern (einschließlich externen IT-Produkten), Objekten, Informationen, Sitzungen und/oder Ressourcen, die verwendet wird, um die SFRs zu definieren, und deren Werte zur Durchsetzung der SFRs verwendet werden

### 3.1.59

#### **Sicherheitsfunktionsrichtlinie**

##### **SFP**

(en: Security Function Policy)

Regelsatz, der ein bestimmtes Sicherheitsverhalten beschreibt, das von der TSF durchgesetzt wird und sich als ein Satz von SFRs beschreiben lässt

### 3.1.60

#### **Sicherheitszielsetzung**

(en: Security Objective)

Absichtserklärung, identifizierte Bedrohungen abzuwehren und/oder identifizierte organisatorische Sicherheitsrichtlinien und/oder -annahmen zu erfüllen

### **3.1.61**

#### **Sicherheitsproblem**

Aussage, die formal die Natur und den Geltungsbereich der Sicherheit definiert, welche den TOE adressieren soll

ANMERKUNG Diese Aussage besteht aus folgenden Teilen:

- den Bedrohungen, die durch den TOE und seine Betriebsumgebung abgewehrt werden sollen,
- den OSPs, die durch den TOE und seine Betriebsumgebung durchgesetzt werden, und
- den Annahmen, die für die Betriebsumgebung des TOEs bestehen.

### **3.1.62**

#### **Sicherheitsanforderung**

in einer standardisierten Sprache ausgedrückte Anforderung, die zur Erreichung der Sicherheitsziele für ein TOE beitragen soll

### **3.1.63**

#### **Sicherheitsvorgabe**

##### **ST**

(en: Security Target)

implementierungsabhängige Beschreibung der Sicherheitsanforderungen für einen spezifischen, identifizierten TOE

### **3.1.64**

#### **Auswahl**

Spezifikation eines oder mehrerer Element(e) aus einer Liste innerhalb einer Komponente

### **3.1.65**

#### **semiformal**

ausgedrückt in einer Sprache mit begrenzter Syntax und definierter Semantik

### **3.1.66**

#### **spezifizieren**

auf stringente und präzise Weise spezifische Einzelheiten zu einer Entität bereitstellen

### **3.1.67**

#### **strikte Konformität**

hierarchische Beziehung zwischen einer ST und einem PP, wobei alle Anforderungen im PP auch in der ST vorhanden sind

ANMERKUNG Diese Beziehung kann grob definiert werden als: „die ST muss alle Aussagen enthalten, die im PP vorhanden sind, darf aber weitere enthalten“. Es wird erwartet, dass strikte Konformität für stringente Anforderungen eingesetzt wird, die in konsistenter Weise erfüllt werden müssen.

### **3.1.68**

#### **ST-Evaluierung**

Bewertung einer ST auf Grundlage definierter Kriterien

### **3.1.69**

#### **Subjekt**

aktive Entität im TOE, die Operationen an Objekten durchführt

### 3.1.70

#### **Evaluierungsgegenstand**

##### **TOE**

(en: Target of Evaluation)

Satz von Software, Firmware und/oder Hardware, möglicherweise mit beigefügten Leitlinien

### 3.1.71

#### **Bedrohungsagent**

Entität, die auf Schutzobjekte nachteilig einwirken kann

### 3.1.72

#### **TOE-Evaluierung**

Bewertung eines TOEs auf Grundlage definierter Kriterien

### 3.1.73

#### **TOE-Ressource**

alles, was innerhalb des TOEs nutzbar oder verwertbar ist

### 3.1.74

#### **TOE-Sicherheitsfunktionalität**

(en: TOE Security Functionality)

kombinierte Funktionalität der gesamten Hardware, Software und Firmware eines TOEs, welche die korrekte Durchsetzung der SFRs sicherstellen muss

### 3.1.75

#### **verfolgen**, Verb

Durchführen einer informalen Korrespondenzanalyse zwischen zwei Entitäten mit nur minimaler Stringenz

### 3.1.76

#### **Übertragungen außerhalb des TOEs**

TSF-vermittelte Kommunikation von Daten an Entitäten, die nicht der Kontrolle der TSF unterliegen

### 3.1.77

#### **Übertragung**

beschreibt den Prozess der Beschreibung von Sicherheitsanforderungen in einer standardisierten Sprache

ANMERKUNG Die Verwendung des Begriffs „Übersetzung“ ist in diesem Zusammenhang nicht wörtlich zu nehmen; es wird nicht impliziert, dass jedes in standardisierter Sprache ausgedrückte SFR wieder in die Sicherheitszielsetzungen zurückübersetzt werden kann.

### 3.1.78

#### **vertrauenswürdiger Kanal**

ein Weg, über den ein TSF und ein anderes vertrauenswürdiges IT-Produkt mit dem notwendigen Vertrauensgrad kommunizieren können

### 3.1.79

#### **vertrauenswürdiges IT-Produkt**

IT-Produkt (nicht der TOE), dessen funktionelle Sicherheitsanforderungen administrativ mit dem TOE koordiniert sind und von dem angenommen wird, dass es die funktionellen Sicherheitsanforderungen korrekt implementiert

ANMERKUNG Ein Beispiel für ein vertrauenswürdiges IT-Produkt wäre ein Produkt, das getrennt evaluiert wurde.

### 3.1.80

#### **vertrauenswürdiger Pfad**

Weg, über den ein Anwender und ein TSF mit dem notwendigen Vertrauensgrad kommunizieren können

### 3.1.81

#### **TSF-Daten**

Daten für den Betrieb des TOEs, welche für die Durchsetzung des SFR benötigt werden

### 3.1.82

#### **TSF-Schnittstelle**

(en: TSF Interface)

Weg, über den externe Entitäten (oder Subjekte im TOE, die nicht Teil des TSF sind) Daten an das TSF übermitteln, Daten vom TSF empfangen und Dienste des TSF aufrufen

### 3.1.83

#### **Benutzerdaten**

Daten für den Benutzer, die nicht den Betrieb des TSF beeinflussen

### 3.1.84

#### **verifizieren**

streng, detailliert und mit einer unabhängig bestimmten Angemessenheit prüfen

ANMERKUNG Siehe auch „bestätigen“. Dieser Begriff hat eine strengere Bedeutung. Der Begriff „verifizieren“ wird im Zusammenhang mit Evaluatorenaktionen verwendet, wenn eine unabhängige Anstrengung durch den Evaluator erforderlich ist.

## 3.2 Begriffe in Zusammenhang mit der Klasse ADV

ANMERKUNG Die folgenden Begriffe werden in den Anforderungen an die interne Software-Struktur verwendet. Einige sind entnommen aus IEEE Standard 610.12-1990, *Standard glossary of software engineering terminology*, Institute of Electrical and Electronics Engineers.

### 3.2.1

#### **Administrator**

Entität, die bezüglich aller durch das TSF implementierten Richtlinien einen Vertrauensgrad besitzt

ANMERKUNG Nicht alle PPs und STs nehmen für Administratoren den gleichen Vertrauensgrad an. Üblicherweise wird angenommen, dass Administratoren jederzeit die in der ST des TOEs definierten Richtlinien einhalten. Manche dieser Richtlinien können mit der Funktionalität des TOEs in Zusammenhang stehen, andere mit der Betriebsumgebung.

### 3.2.2

#### **Aufrufbaum**

identifiziert die Module in einem System in Form eines Diagramms, das aufzeigt, welche Module sich gegenseitig aufrufen

ANMERKUNG Basierend auf IEEE Standard 610.12-1990.

### 3.2.3

#### **Kohäsion**

Modulstärke

Art und Grad, wie die von einem Software-Modul durchgeführten Aufgaben miteinander in Zusammenhang stehen

[IEEE Standard 610.12-1990]

ANMERKUNG Zu den Kohäsionsarten gehören die zufällige, die kommunikative, die funktionelle, die logische, die sequentielle und die zeitliche Kohäsion. Diese Kohäsionsarten werden beim entsprechenden Begriffseintrag beschrieben.

### 3.2.4

#### **zufällige Kohäsion**

Modul, das unzusammenhängende oder nur bedingt zusammenhängende Aktivitäten ausführt

[IEEE Standard 610.12-1990]

ANMERKUNG Siehe auch Kohäsion (3.2.3).

### 3.2.5

#### **kommunikative Kohäsion**

Modul, das Funktionen enthält, die Ausgaben für andere Funktionen innerhalb des Moduls produzieren oder Ausgaben anderer Funktionen innerhalb des Moduls nutzen

[IEEE Standard 610.12-1990]

ANMERKUNG 1 Siehe auch Kohäsion (3.2.3).

ANMERKUNG 2 Ein Beispiel für ein kommunikativ kohäsives Modul ist ein Zugriffsüberprüfungsmodul, das obligatorische, diskrete und Funktionsprüfungen enthält.

### 3.2.6

#### **Komplexität**

Maßwert dafür, wie schwierig Software zu verstehen und daher zu analysieren, testen und warten ist

[IEEE Standard 610.12-1990]

ANMERKUNG Die Reduzierung der Komplexität ist das oberste Ziel beim Einsatz von modularer Aufteilung, Schichtung und Minimierung. Die Kontrolle von Kopplung und Kohäsion trägt erheblich zur Erreichung dieses Ziels bei.

Im Bereich des Software-Engineering wurde erheblicher Aufwand in den Versuch investiert, Metriken zur Messung der Komplexität von Quellcode zu entwickeln. Die meisten dieser Metriken nutzen einfach zu berechnende Eigenschaften des Quellcodes, wie beispielsweise die Anzahl von Operatoren und Operanden, die Komplexität des Kontrollflussgraphen (zyklomatische Komplexität), die Anzahl der Quellcode-Zeilen, das Verhältnis zwischen Kommentaren und ausführbarem Code und ähnliche Maßwerte. Kodierungsstandards haben sich als wertvolles Instrument zur Erzeugung von Code erwiesen, der einfacher zu verstehen ist.

Die Familie der TSF-Interna (ADV\_INT) erfordert eine Komplexitätsanalyse aller Komponenten. Es wird erwartet, dass der Entwickler Nachweise für die Behauptung liefert, dass die Komplexität ausreichend reduziert wurde. Diese Nachweise können beispielsweise die Programmierstandards des Entwicklers enthalten sowie eine Angabe, dass alle Module den Standards entsprechen (oder dass es einige Ausnahmen gibt, die durch Software-Engineering-Argumente begründet sind). Sie könnten die Ergebnisse von Werkzeugen enthalten, die zur Messung mancher Eigenschaften des Quellcodes eingesetzt wurden, oder andere Nachweise, die der Entwickler für angemessen hält.

### 3.2.7

#### **Kopplung**

Art und Grad der gegenseitigen Abhängigkeit von Software-Modulen

[IEEE Standard 610.12-1990]

ANMERKUNG Zu den Kopplungsarten gehören die Aufrufkopplung, die Bereichskopplung und die Inhaltskopplung. Diese sind nachstehend beschrieben.

### 3.2.8

#### **Aufrufkopplung**

Beziehung zwischen zwei Modulen, die strikt nur über ihre dokumentierten Funktionsaufrufe kommunizieren

ANMERKUNG Beispiele für die Aufrufkopplung sind die Daten-, Datenstruktur- und Kontrollkopplung.

### **3.2.9**

#### **Aufrufkopplung**

<Datenkopplung> Beziehung zwischen zwei Modulen, die strikt nur durch die Verwendung von Aufrufparametern kommunizieren, die einzelnen Datenelementen entsprechen

ANMERKUNG Siehe auch Aufrufkopplung (3.2.8).

### **3.2.10**

#### **Aufrufkopplung**

<Datenstrukturkopplung> Beziehung zwischen zwei Modulen, die durch die Verwendung von Aufrufparametern kommunizieren, die mehrere Felder umfassen oder die sinnvolle interne Strukturen haben

ANMERKUNG Siehe auch Aufrufkopplung (3.2.8).

### **3.2.11**

#### **Aufrufkopplung**

<Kontrollkopplung> Beziehung zwischen zwei Modulen, wobei ein Modul Informationen weitergibt, welche die interne Logik des anderen Moduls beeinflussen sollen

ANMERKUNG Siehe auch Aufrufkopplung (3.2.8).

### **3.2.12**

#### **Bereichskopplung**

Beziehung zwischen zwei Modulen, die sich einen gemeinsamen Datenbereich oder eine andere gemeinsame Systemressource teilen

ANMERKUNG Globale Variablen zeigen an, dass die Module, die diese globalen Variablen verwenden, über eine Bereichskopplung verfügen. Die Bereichskopplung mittels globaler Variablen ist allgemein zulässig, aber nur in einem begrenzten Ausmaß.

Beispielsweise sind Variablen, die in einem globalen Bereich platziert sind, aber nur von einem einzigen Modul verwendet werden, unpassend platziert und sollten entfernt werden. Weitere Faktoren, die bei der Bewertung der Eignung globaler Variablen berücksichtigt werden müssen, sind:

Die Anzahl der Module, die eine globale Variable modifizieren: Im Allgemeinen sollte nur ein einziges Modul die Kontrolle des Inhalts einer globalen Variablen wahrnehmen, aber es kann Situationen geben, in denen ein zweites Modul diese Aufgabe ebenfalls wahrnimmt; in solchen Fällen muss eine ausreichende Begründung geliefert werden. Es ist nicht annehmbar, dass diese Aufgabe von mehr als zwei Modulen wahrgenommen wird. (Bei der Durchführung dieser Bewertung sollte sorgfältig bestimmt werden, welches Modul tatsächlich für den Inhalt der Variablen verantwortlich ist. Wenn die Variable beispielsweise nur von einer Routine modifiziert wird, aber diese Routine einfach nur die vom aufrufenden Modul angeforderte Modifikation durchführt, dann ist das aufrufende Modul verantwortlich, und es könnten mehrere solcher Module vorhanden sein). Wenn zwei Module für den Inhalt einer globalen Variablen zuständig sind, sollte des Weiteren als Teil der Komplexitätsbewertung klar definiert sein, wie die Modifikationen zwischen den Modulen koordiniert werden.

Die Anzahl der Module, die eine globale Variable referenzieren: Auch wenn es keinen allgemeinen Grenzwert für die Anzahl der Module gibt, die eine globale Variable referenzieren, sollte in Fällen, in denen viele Module eine solche Referenzierung durchführen, die Gültigkeit und Notwendigkeit untersucht werden.

### **3.2.13**

#### **Inhaltskopplung**

Beziehung zwischen zwei Modulen, wobei ein Modul die Interna des anderen Moduls direkt referenziert

ANMERKUNG Beispiele sind die Modifizierung des Codes oder die Referenzierung von internen Labels des anderen Moduls. Daraus ergibt sich, dass ein Teil oder der gesamte Inhalt eines Moduls effektiv im anderen Modul enthalten ist. Die Inhaltskopplung kann als die Verwendung nicht offengelegter Modulschnittstellen betrachtet werden, im Gegensatz zur Aufrufkopplung, bei der nur offengelegte Modulschnittstellen verwendet werden.

### 3.2.14

#### **Domänentrennung**

Eigenschaft von Sicherheitsarchitekturen, wobei das TSF getrennte Sicherheitsdomänen für jeden Benutzer und für das TSF definiert und sicherstellt, dass kein Benutzerprozess den Inhalt der Sicherheitsdomäne eines anderen Benutzers oder des TSF beeinflussen kann

### 3.2.15

#### **funktionelle Kohäsion**

funktionelle Eigenschaft eines Moduls, das nur Aktivitäten für eine einzige Aufgabe durchführt

[IEEE Standard 610.12-1990]

ANMERKUNG Ein funktionell kohäsives Modul wandelt eine einzige Eingabeart in eine einzige Ausgabeart um, wie beispielsweise ein Stack-Manager oder ein Warteschlangen-Manager. Siehe auch Kohäsion (3.2.3).

### 3.2.16

#### **Interaktion**

allgemeine, auf Kommunikation basierende Aktivität zwischen Entitäten

### 3.2.17

#### **Schnittstelle**

Mittel zur Interaktion mit einer Komponente oder einem Modul

### 3.2.18

#### **Schichtung**

Entwurfstechnik, bei der getrennte Modulgruppen (die Schichten) hierarchisch so organisiert sind, dass sie getrennte Zuständigkeiten besitzen, wobei eine Schicht nur die Dienste der in der Hierarchie darunterliegenden Schichten nutzt und die eigenen Dienste nur den darüberliegenden Schichten zur Verfügung stellt

ANMERKUNG Bei einer strengen Schichtung gilt zusätzlich, dass jede Schicht nur die Dienste der unmittelbar darunterliegenden Schicht nutzen kann und ihre Dienste nur für die unmittelbar darüberliegende Schicht zur Verfügung stellt.

### 3.2.19

#### **logische Kohäsion**

#### **prozedurale Kohäsion**

Merkmale eines Moduls, das ähnliche Aktivitäten an verschiedenen Datenstrukturen durchführt

ANMERKUNG Ein Modul weist eine logische Kohäsion auf, wenn seine Funktionen verwandte, aber unterschiedliche Operationen an verschiedenen Eingaben durchführen. Siehe auch „Kohäsion“.

### 3.2.20

#### **modulare Aufteilung**

Prozess der Aufteilung eines Systems in Komponenten, um den Entwurf, die Entwicklung und die Evaluierung zu vereinfachen

[IEEE Standard 610.12-1990]

### 3.2.21

#### **Unumgänglichkeit**

<des TSF> Eigenschaft einer Sicherheitsarchitektur, wobei alle Aktionen in Zusammenhang mit dem SFR vom TSF vermittelt werden

### **3.2.22**

#### **Sicherheitsdomänen**

Umgebungen, die vom TSF für die Nutzung durch nicht vertrauenswürdige Entitäten derart bereitgestellt werden, dass diese Umgebungen isoliert und voreinander geschützt sind

### **3.2.23**

#### **sequentielle Kohäsion**

Modul, das Funktionen enthält, deren Ausgaben als Eingaben für die jeweils folgenden Funktionen innerhalb des Moduls genutzt werden

[IEEE Standard 610.12-1990]

**ANMERKUNG** Ein Beispiel für ein sequentiell-kohäsives Modul ist ein Modul, das Funktionen zum Schreiben von Audit-Datensätzen und zur laufenden Zählung einer spezifischen Art von akkumulierten Audit-Verletzungen enthält.

### **3.2.24**

#### **Software-Engineering**

Einsatz eines systematischen, disziplinierten und quantifizierbaren Verfahrens zur Entwicklung und Wartung von Software; kurz die Anwendung von Ingenieurwissenschaften auf Software

[IEEE Standard 610.12-1990]

**ANMERKUNG** Wie bei allen ingenieurwissenschaftlichen Praktiken ist bei der Anwendung der Engineering-Prinzipien ein gewisses Urteilsvermögen nötig. Entscheidungen werden durch eine Vielzahl von Faktoren beeinflusst, nicht nur durch die Anwendung von Maßnahmen zur modularen Aufteilung, Schichtung und Minimierung. So kann ein Entwickler beispielsweise ein System entwerfen, bei dem er zukünftige Applikationen berücksichtigt, die anfänglich nicht implementiert werden. Der Entwickler kann daher Logik einbinden, um diese zukünftigen Applikationen zu handhaben, ohne sie vollständig zu implementieren; des Weiteren kann der Entwickler Aufrufe von bisher nicht implementierten Modulen einschließen, so dass unvollständige Aufrufe (en: Call Stubs) entstehen. Bei der Beurteilung, ob solche Abweichungen von gut strukturierten Programmen durch den Entwickler gerechtfertigt sind, muss Urteilsvermögen und eine gute Software-Engineering-Disziplin zur Anwendung kommen.

### **3.2.25**

#### **zeitliche Kohäsion**

Merkmal eines Moduls, das Funktionen enthält, die ungefähr gleichzeitig ausgeführt werden müssen

**ANMERKUNG 1** Basierend auf [IEEE Standard 610.12-1990].

**ANMERKUNG 2** Beispiele für zeitlich kohäsive Module sind Module für die Initialisierung, Wiederherstellung und Abschaltung.

### **3.2.26**

#### **TSF-Selbstschutz**

Eigenschaft einer Sicherheitsarchitektur, wobei das TSF nicht von TSF-fremdem Code oder fremden Entitäten beschädigt werden kann

## **3.3 Begriffe in Zusammenhang mit der Klasse AGD**

### **3.3.1**

#### **Installation**

von einem menschlichen Benutzer durchgeführtes Verfahren zur Einbindung des TOEs in seine Betriebsumgebung und dessen Inbetriebnahme

**ANMERKUNG** Diese Operation wird normalerweise nur einmal nach Erhalt und Abnahme des TOEs durchgeführt. Es wird erwartet, dass der TOE soweit konfiguriert wird, dass die Konfiguration entsprechend der ST zulässig ist. Wenn ähnliche Prozesse durch den Entwickler durchgeführt werden müssen, dann werden sie im Rahmen der ALC: Produktlebenszyklusunterstützung als „Generierung“ bezeichnet. Falls der TOE eine Erstinbetriebnahme erfordert, die nicht regelmäßig wiederholt werden muss, dann würde dieser Prozess als Installation eingestuft.