DIN EN ISO/IEC 15408-5

DIN

ICS 35.030

Einsprüche bis 2024-01-10

Entwurf

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Evaluationskriterien für IT-Sicherheit – Teil 5: Vordefinierte Pakete von Sicherheitsanforderungen (ISO/IEC 15408-5:2022); Deutsche und Englische Fassung prEN ISO/IEC 15408-5:2023

Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 5: Pre-defined packages of security requirements (ISO/IEC 15408-5:2022); German and English version prEN ISO/IEC 15408-5:2023

Sécurité de l'information, cybersécurité et protection de la vie privée – Critères d'évaluation pour la sécurité des technologies de l'information – Partie 5: Paquets prédéfinis d'exigences de sécurité (ISO/IEC 15408-5:2022); Version allemande et anglaise prEN ISO/IEC 15408-5:2023

Anwendungswarnvermerk

Dieser Entwurf mit Erscheinungsdatum 2023-11-10 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil das beabsichtigte Dokument von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

— vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;

— oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;

— oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Es wird gebeten, mit den Kommentaren zu diesem Entwurf jegliche relevanten Patentrechte, die bekannt sind, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 73 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

Nationales Vorwort

Der Text von ISO/IEC 15408-5:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 15408-5:2023 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 Gemeinschaftsarbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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

ISO/IEC 15408-1:2022 siehe DIN EN ISO/IEC 15408-1:2024-02*

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

* Zurzeit Entwurf.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO/IEC 15408-1:2024-02, *Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit — Teil 1: Einführung und allgemeines Modell*

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

– Leerseite –

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

– Entwurf –

Juli 2023

prEN ISO/IEC 15408-5

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Evaluationskriterien für IT-Sicherheit – Teil 5: Vordefinierte Pakete von Sicherheitsanforderungen (ISO/IEC 15408-5:2022)

Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 5: Pre-defined packages of security requirements (ISO/IEC 15408-5:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée – Critères d'évaluation pour la sécurité des technologies de l'information – Partie 5: Paquets prédéfinis d'exigences de sécurité (ISO/IEC 15408-5:2022)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

Inhalt

Seite

Europäisches Vorwort 4
Vorwort 5
Einleitung 7
1 Anwendungsbereich 8
2 Normative Verweisungen 8
3 Begriffe 8
4 Vertrauenswürdigkeitsstufen 9
4.1 Name der Familie 9
4.2 Überblick über die Vertrauenswürdigkeitsstufen 9
4.2.1 Allgemeines 9
4.2.2 Beziehung zwischen Vertrauenswürdigkeiten und Vertrauenswürdigkeitsstufen 9
4.3 Zielsetzungen der Vertrauenswürdigkeitsstufen 11
4.4 Vertrauenswürdigkeitsstufen 12
4.4.1 Allgemeines 12
4.4.2 Vertrauenswürdigkeitsstufe 1 (EAL1) — Funktionell geprüft 12
4.4.3 Vertrauenswürdigkeitsstufe 2 (EAL2) — Strukturell geprüft 13
4.4.4 Vertrauenswürdigkeitsstufe 3 (EAL3) — Methodisch geprüft und kontrolliert 15
4.4.5 Vertrauenswürdigkeitsstufe 4 (EAL4) — Methodisch gestaltet, geprüft und bewertet . . . 16
4.4.6 Vertrauenswürdigkeitsstufe 5 (EAL5) — Semiformal verifiziert, gestaltet und geprüft . . 18
4.4.7 Vertrauenswürdigkeitsstufe 6 (EAL6) — Semiformal verifiziertes Design und geprüft . . 19
4.4.8 Vertrauenswürdigkeitsstufe 7 (EAL7) — Formal verifiziertes Design und geprüft 21
5 Zusammengesetzte Vertrauenswürdigkeitspakete (CAP) 23
5.1 Name der Familie 23
5.2 Überblick über zusammengesetzte Vertrauenswürdigkeitspakete (CAP) 23
5.2.1 Allgemeines 23
5.2.2 Beziehung zwischen Vertrauenswürdigkeiten und Vertrauenswürdigkeitspaketen 23
5.3 Zielsetzungen des zusammengesetzten Vertrauenswürdigkeitspakets (CAP) 24
5.4 Pakete in der CAP-Familie 26
5.4.1 Zusammengesetztes Vertrauenswürdigkeitspaket A — strukturell zusammengesetzt . . 26
5.4.2 Zusammengesetztes Vertrauenswürdigkeitspaket B — Methodisch zusammengesetzt . . 27
5.4.3 Zusammengesetztes Vertrauenswürdigkeitspaket C — Methodisch zusammengesetzt, geprüft und bewertet 29
6 Verbundproduktpaket 30
6.1 Paketname 30
6.2 Pakettyp 30
6.3 Paketüberblick 30
6.4 Zielsetzungen 30
6.5 Vertrauenswürdigkeitskomponenten 31
7 Vertrauenswürdigkeiten für das Schutzprofil 31
7.1 Name der Familie 31
7.2 Überblick über die PPA-Familie 31
7.3 Zielsetzungen der PPA-Familie 32
7.4 PPA-Pakete 32
7.4.1 Vertrauenswürdigkeitspaket für das Schutzprofil — PP mit direkter Begründung 32
7.4.2 Vertrauenswürdigkeitspaket für das Schutzprofil — Standard 33
8 Vertrauenswürdigkeiten für die Sicherheitsvorgabe 34
8.1 Name der Familie 34
8.2 Überblick über die STA-Familie 34
8.3 Zielsetzungen der STA-Familie 34
8.4 STA-Pakete 34
8.4.1 Vertrauenswürdigkeitspaket für die Sicherheitsvorgabe — Direkte Begründung 34

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

8.4.2 Vertrauenswürdigkeitspaket für die Sicherheitsvorgabe — Standard 35

Bilder

Bild 1 — Zusammenhang zwischen Vertrauenswürdigkeit und Vertrauenswürdigkeitsstufe . . . 10
Bild 2 — Zusammenhang zwischen der Vertrauenswürdigkeit und dem zusammengesetzten Vertrauenswürdigkeitspaket (CAP) 24

Tabellen

Tabelle 1 — Zusammenfassung der Vertrauenswürdigkeitsstufen 11
Tabelle 2 — EAL1 13
Tabelle 3 — EAL2 14
Tabelle 4 — EAL3 15
Tabelle 5 — EAL4 17
Tabelle 6 — EAL5 19
Tabelle 7 — EAL6 20
Tabelle 8 — EAL7 22
Tabelle 9 — Zusammenfassung des zusammengesetzten Vertrauenswürdigkeitspaket 26
Tabelle 10 — CAP-A 27
Tabelle 11 — CAP-B 28
Tabelle 12 — CAP-C 30
Tabelle 13 — COMP 31
Tabelle 14 — PPA-Zusammenfassung 32
Tabelle 15 — PPA-DR 33
Tabelle 16 — PPA-STD 33
Tabelle 17 — STA-Zusammenfassung 34
Tabelle 18 — STA-DR 35
Tabelle 19 — STA-STD 36

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

Europäisches Vorwort

Der Text von ISO/IEC 15408-5:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ als prEN ISO/IEC 15408-5:2023 übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Anerkennungsnotiz

Der Text von ISO/IEC 15408-5:2022 wurde von CEN als prEN ISO/IEC 15408-5:2023 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

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.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC Directives, Teil 1, beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC Directives, Teil 2, erarbeitet (siehe www.iso.org/directives oder www.iec.ch/members_experts/refdocs).

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. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents) oder in der IEC-Liste der erhaltenen Patenterklärungen (siehe https://patents.iec.ch).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html. In der IEC, siehe www.iec.ch/understanding-standards.

Dieses Dokument wurde vom Technischen Komitee ISO/TC JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection,* erarbeitet.

Eine Auflistung aller Teile der Normenreihe ISO/IEC 15408 kann auf der ISO-Internetseite abgerufen werden.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html und www.iec.ch/national-committees zu finden.

AVA Documents Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

Rechtliche Hinweise

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 (kurz CC) erteilen sie hiermit der ISO/IEC die nicht-exklusive Lizenz zur Verwendung der CC für die weitere Entwicklung/Pflege der Normenreihe ISO/IEC 15408. Diese Regierungsorganisationen behalten sich allerdings das Recht zur Nutzung, Vervielfältigung, zum Vertrieb sowie zur Übersetzung und Änderung der CC nach Belieben vor.

Australien	The Australian Signals Directorate
Kanada	Communications Security Establishment
Frankreich	Agence Nationale 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
Neuseeland	Government Communications Security Bureau
Republik Korea	National Security Research Institute
Spanien	Ministerio de Asuntos Económicos y Transformación Digital
Schweden	FMV, Swedish Defence Materiel Administration
Vereinigtes Königreich	National Cyber Security Centre
USA	The National Security Agency

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

Einleitung

Dieses Dokument enthält vordefinierte Pakete von Sicherheitsanforderungen. Solche Sicherheitsanforderungen können für interessierte Parteien nützlich sein, wenn sie die Konformität zwischen Evaluierungen anstreben. Pakete von Sicherheitsanforderungen können auch dazu beitragen, den Aufwand für die Entwicklung von Schutzprofilen (PP) und Sicherheitsvorgaben (ST) zu verringern.

ISO/IEC 15408-1 definiert den Begriff „Paket“ und beschreibt die grundlegenden Konzepte.

ANMERKUNG Im vorliegenden Dokument werden einige Begriffe fett und kursiv gedruckt, um sie vom übrigen Text abzuheben. Die Beziehung zwischen den Komponenten einer Familie wird als Konvention über eine Fettmarkierung hervorgehoben. Diese Markierungskonvention erfordert die Verwendung von Fettdruck für alle neuen Anforderungen. Für hierarchische Komponenten werden Anforderungen fett hervorgehoben, wenn sie über die Anforderungen der vorherigen Komponente hinaus erweitert oder geändert werden. Zusätzlich werden alle neuen oder erweiterten zulässigen, über die vorherige Komponente hinausgehenden Operationen ebenfalls fett hervorgehoben.

Die Verwendung von Kursivschrift weist auf einen Text hin, der eine genaue Bedeutung hat. Für die Vertrauenswürdigkeitsanforderungen gilt die Konvention für spezielle Verben, die sich auf die Evaluierung beziehen.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

1 Anwendungsbereich

Dieses Dokument enthält Pakete von Vertrauenswürdigkeits- und Sicherheitsfunktionsanforderungen, die als zweckmäßig zur Unterstützung der gemeinsamen Nutzung durch die interessierten Parteien identifiziert worden sind.

BEISPIEL Beispiele für bereitgestellte Pakete umfassen die Vertrauenswürdigkeitsstufen (EAL-Stufen) und die zusammengesetzten Vertrauenswürdigkeitspakete (CAP).

Dieses Dokument zeigt Folgendes:

— Familie von Paketen für *Vertrauenswürdigkeitsstufen (EAL)*, die vordefinierte Sätze von Vertrauenswürdigkeitskomponenten festlegen, auf die in den PP und ST verwiesen werden darf und die geeignete, während einer Evaluierung eines Evaluierungsgegenstands (TOE) zu erbringende Vertrauenswürdigkeiten spezifizieren;

— Familie von *zusammengesetzten Vertrauenswürdigkeitspaketen (CAP)*, die Sätze von Vertrauenswürdigkeitskomponenten spezifizieren, die zur Spezifikation geeigneter, während einer Evaluierung zusammengesetzter TOE zu erbringender Sicherheitszusicherungen verwendet werden;

— *Paket aus einem Verbundprodukt (COMP)*, das einen Satz von Vertrauenswürdigkeitskomponenten festlegt. Diese müssen zur Spezifikation geeigneter Vertrauenswürdigkeiten verwendet werden und während einer Evaluierung eines aus einem Verbundprodukt bestehenden TOE bereitgestellt werden;

— Paketfamilie von *Schutzprofilzusicherungen (PPA)*, die Sätze von Vertrauenswürdigkeitskomponenten spezifizieren, die zur Spezifikation geeigneter, während einer Schutzprofilevaluierung zu erbringender Vertrauenswürdigkeiten verwendet werden;

— Paketfamilie von *Sicherheitsvorgabezusicherungen (STA)*, die Sätze von Vertrauenswürdigkeitskomponenten spezifizieren, die zur Spezifikation geeigneter Vertrauenswürdigkeiten verwendet werden und während einer Evaluierung der Sicherheitsvorgaben zu erbringen sind.

Zu den Benutzern dieses Dokuments können Verbraucher, Entwickler und Evaluatoren von sicheren IT-Produkten gehören.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. 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 15408-1:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-3:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe und Abkürzungen nach ISO/IEC 15408-1 und ISO/IEC 15408-3.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— ISO Online Browsing Platform: verfügbar unter https://www.iso.org/obp

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

— IEC Electropedia: verfügbar unter https://www.electropedia.org/

4 Vertrauenswürdigkeitsstufen

4.1 Name der Familie

Der Name dieser Paketfamilie lautet „Evaluation assurance levels“ (EAL).

4.2 Überblick über die Vertrauenswürdigkeitsstufen

4.2.1 Allgemeines

Die EAL bieten eine aufsteigende Skala, die sowohl die erreichte Vertrauenswürdigkeitsstufe als auch die Kosten zur Erlangung dieser Vertrauenswürdigkeitsstufe und die Durchführbarkeit berücksichtigt. Der Ansatz von ISO/IEC 15408-1 identifiziert die getrennten Konzepte der Vertrauenswürdigkeit eines TOE am Ende der Evaluierung und der Aufrechterhaltung dieser Vertrauenswürdigkeit während der betrieblichen Nutzung des TOE.

ANMERKUNG Nicht alle in ISO/IEC 15408-3 aufgeführten Familien und Komponenten sind in den EAL enthalten. Das soll nicht heißen, dass diese keine sinnvollen und wünschenswerten Vertrauenswürdigkeiten bieten. Stattdessen wird erwartet, dass diese Familien und Komponenten für die Ergänzung einer EAL in denjenigen Schutzprofilen (PP) und Sicherheitsvorgaben (ST) in Betracht gezogen werden können, für die sie von Nutzen sind. Außerdem sind einige der in ISO/IEC 15408-3 enthaltenen Klassen für die EAL nicht relevant. Beispiele für solche Klassen umfassen die Klassen APE und ACO.

Für jede EAL wurde ein Satz von Vertrauenswürdigkeitskomponenten ausgewählt.

Eine höhere Vertrauenswürdigkeitsstufe als die einer bestimmten EAL kann erreicht werden durch:

a) Einbeziehung zusätzlicher Vertrauenswürdigkeitskomponenten aus anderen Vertrauenswürdigkeitsfamilien; oder

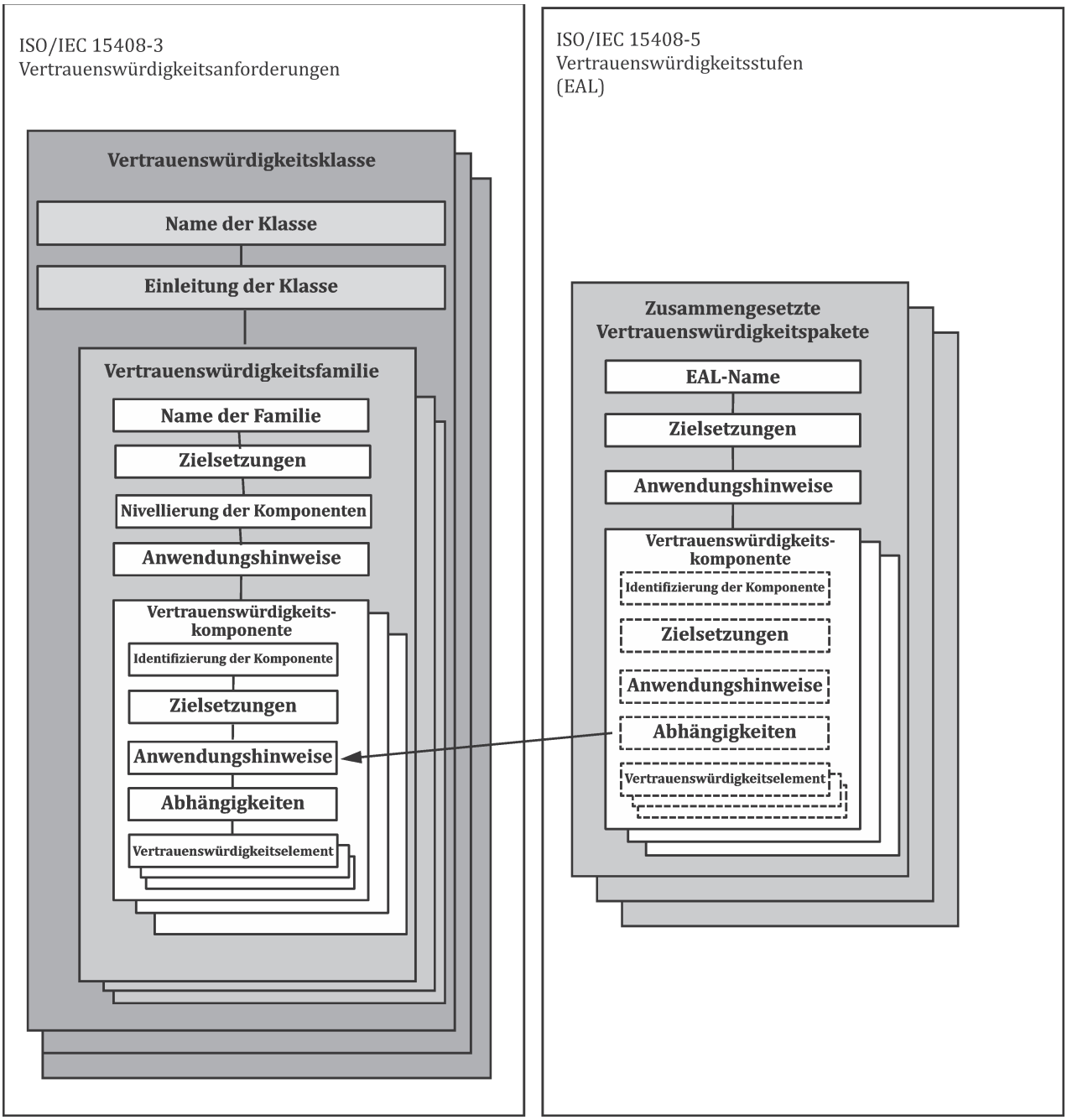
b) Ersetzung einer Vertrauenswürdigkeitskomponente durch eine übergeordnete Vertrauenswürdigkeitskomponente aus derselben Vertrauenswürdigkeitsfamilie.

4.2.2 Beziehung zwischen Vertrauenswürdigkeiten und Vertrauenswürdigkeitsstufen

Bild 1 veranschaulicht die Beziehung zwischen den in ISO/IEC 15408-3 enthaltenen Vertrauenswürdigkeitsanforderungen (SAR) und den in diesem Dokument definierten Vertrauenswürdigkeitsstufen. Während Vertrauenswürdigkeitskomponenten weiter in Vertrauenswürdigkeitselemente zerlegt werden, kann auf Vertrauenswürdigkeitselemente nicht einzeln durch Vertrauenswürdigkeitsstufen verwiesen werden.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12



ANMERKUNG Der Pfeil im Bild stellt eine Verweisung von einer EAL zu einer Vertrauenswürdigkeitskomponente innerhalb der Klasse dar, in der sie definiert ist.

Bild 1 — Zusammenhang zwischen Vertrauenswürdigkeit und Vertrauenswürdigkeitsstufe

Tabelle 1 enthält eine Zusammenfassung der EAL. Die Spalten stehen für eine hierarchisch geordnete Menge von EAL, während die Zeilen für Vertrauenswürdigkeitsfamilien stehen. Jede Zahl in der sich daraus ergebenden Matrix identifiziert gegebenenfalls eine bestimmte Vertrauenswürdigkeitskomponente.

Die grau markierten Punkte sind in der EAL-Spezifikation nicht anwendbar. Sie können jedoch zur Ergänzung des EAL-Pakets verwendet werden.

ANMERKUNG Obwohl die ALC_FLR- und ALC_TDA-Familien nicht in Tabelle 1 aufgeführt sind, werden sie häufig als Ergänzung zu den EAL verwendet.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

Tabelle 1 — Zusammenfassung der Vertrauenswürdigkeitsstufen

Vertrauenswürdigkeits-klasse	Vertrauens-würdigkeits-familie	Vertrauenswürdigkeitskomponenten je 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
Lebenszyklusunterstützung	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_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
ST-Evaluierung	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
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

4.3 Zielsetzungen der Vertrauenswürdigkeitsstufen

Wie in 4.4 dargelegt, werden in diesem Dokument sieben hierarchisch geordnete Vertrauenswürdigkeitsstufen für die Bewertung der Vertrauenswürdigkeit eines TOE definiert. Sie sind insofern hierarchisch geordnet, als jede EAL mehr Vertrauenswürdigkeit darstellt als alle niedrigeren EAL. Die Erhöhung der Vertrauenswürdigkeit von EAL zu EAL wird durch den Austausch einer hierarchisch höheren Vertrauenswürdigkeitskomponente aus derselben Vertrauenswürdigkeitsfamilie (d. h. Erhöhung der Stringenz, des Anwendungsbereichs und/oder der Tiefe) und durch das Hinzufügen von Vertrauenswürdigkeitskomponenten aus anderen Vertrauenswürdigkeitsfamilien (d. h. Hinzufügen neuer Anforderungen) erreicht.

Diese EAL bestehen aus einer geeigneten Kombination von Vertrauenswürdigkeitskomponenten, wie in ISO/IEC 15408-3 beschrieben. Genauer gesagt, umfasst jede EAL nicht mehr als eine Komponente jeder

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

Vertrauenswürdigkeitsfamilie und alle Vertrauenswürdigkeitsabhängigkeiten jeder Komponente werden berücksichtigt.

Der Begriff der „Ergänzung“ erlaubt die Hinzufügung von Vertrauenswürdigkeitskomponenten (aus Vertrauenswürdigkeitsfamilien, die noch nicht in der EAL enthalten sind) oder den Austausch von Vertrauenswürdigkeitskomponenten (durch eine andere, hierarchisch höhere Vertrauenswürdigkeitskomponente aus derselben Vertrauenswürdigkeitsfamilie) in einer EAL. Von den in ISO/IEC 15408-1 definierten Vertrauenswürdigkeitskonstrukten dürfen nur die EAL ergänzt werden. Der Begriff „EAL abzüglich einer einen Bestandteil bildenden Vertrauenswürdigkeitskomponente“ wird in ISO/IEC 15408-1 nicht als gültiger Anspruch anerkannt. Für den Anspruchsteller geht mit einer Ergänzung die Verpflichtung einher, den Nutzen und den Mehrwert der zusätzlichen Vertrauenswürdigkeitskomponente für die EAL zu begründen. Eine EAL darf auch durch erweiterte Vertrauenswürdigkeitsanforderungen ergänzt werden.

ANMERKUNG Eine EAL kann nicht ergänzt werden, wenn sie in einer ST enthalten ist, die genaue Konformität mit einem PP beansprucht.

4.4 Vertrauenswürdigkeitsstufen

4.4.1 Allgemeines

Dieser Unterabschnitt enthält Definitionen der EAL, wobei die Unterschiede zwischen den spezifischen Anforderungen und den Prosabeschreibungen dieser Anforderungen durch Fettdruck hervorgehoben werden.

4.4.2 Vertrauenswürdigkeitsstufe 1 (EAL1) — Funktionell geprüft

4.4.2.1 Paketname

Der Name des Pakets lautet „Evaluation assurance level 1“ (EAL1) — funktionell geprüft.

4.4.2.2 Pakettyp

Dies ist ein Vertrauenswürdigkeitspaket.

4.4.2.3 Paketüberblick

EAL1 ist anwendbar, wenn ein gewisses Maß an Vertrauen in den korrekten Betrieb erforderlich ist, die Bedrohungen für die Sicherheit aber nicht als ernsthaft angesehen werden. Sie ist von Wert, wenn eine unabhängige Vertrauenswürdigkeit erforderlich ist, um das Argument zu untermauern, dass in Bezug auf den Schutz personenbezogener oder ähnlicher Daten gebührende Sorgfalt angewandt wurde.

EAL1 erfordert nur eine begrenzte ST. Es reicht aus, die geforderten Sicherheitsfunktionsanforderungen (SFR) für den TOE anzugeben, anstatt sie aus Bedrohungen, organisatorischen Sicherheitsrichtlinien (OSP) und Annahmen durch Sicherheitszielsetzungen abzuleiten.

EAL1 bietet eine Evaluierung des TOE, wie er dem Kunden zur Verfügung gestellt wird, einschließlich unabhängiger Prüfungen anhand einer Spezifikation und einer Untersuchung der zur Verfügung gestellten Leitliniendokumentation. Es ist vorgesehen, dass eine EAL1-Evaluierung ohne Unterstützung durch den Entwickler des TOE und mit minimalem Aufwand erfolgreich durchgeführt werden kann.

Eine Evaluierung auf dieser Stufe erbringt den Nachweis, dass der TOE in einer mit seiner Dokumentation konsistenten Weise funktioniert.

4.4.2.4 Zielsetzungen des Pakets

EAL1 bietet eine niedrige Vertrauenswürdigkeitsstufe durch eine begrenzte ST und eine Analyse der SFR in dieser ST unter Verwendung einer Funktions- und Schnittstellenspezifikation und einer Leitliniendokumentation, um das Sicherheitsverhalten zu verstehen.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

Die Analyse wird durch eine Suche nach potentiellen Anfälligkeiten im öffentlichen Bereich und durch unabhängige Prüfung (Funktions- und Penetrationsprüfung) der TOE-Sicherheitsfunktionalität (TSF) unterstützt.

EAL1 bietet auch Vertrauenswürdigkeit durch eindeutige Identifizierung des TOE und der relevanten Evaluierungsdokumente.

Diese EAL bietet einen bedeutenden Zuwachs an Vertrauenswürdigkeit gegenüber nicht evaluierter IT.

4.4.2.5 Vertrauenswürdigkeitskomponenten

In Tabelle 2 sind die in EAL 1 enthaltenen Vertrauenswürdigkeitskomponenten aufgeführt.

Tabelle 2 — EAL1

Vertrauenswürdigkeitsklasse	Vertrauenswürdigkeitskomponenten
ADV: Entwicklung	ADV_FSP.1 Basic functional specification
AGD: Leitliniendokumente	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Lebenszyklusunterstützung	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: ST-Evaluierung	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Prüfungen	ATE_IND.1 Independent testing – conformance
AVA: Anfälligkeitsbewertung	AVA_VAN.1 Vulnerability survey

4.4.3 Vertrauenswürdigkeitsstufe 2 (EAL2) — Strukturell geprüft

4.4.3.1 Paketname

Der Name des Pakets lautet „Evaluation assurance level 2“ (EAL2) — strukturell geprüft.

4.4.3.2 Pakettyp

Dies ist ein Vertrauenswürdigkeitspaket.

4.4.3.3 Paketüberblick

EAL2 erfordert die Mitwirkung des Entwicklers bei der Bereitstellung von Designinformationen und Prüfungsergebnissen, sollte ihm aber nicht mehr Aufwand abverlangen, als mit guter Geschäftspraxis vereinbar ist. Als solche sollte sie keine wesentlich höheren Investitionen an Kosten oder Zeit erfordern.

EAL2 ist daher in den Fällen anwendbar, in denen Entwickler oder Benutzer eine geringe bis mittlere Stufe unabhängig garantierter Sicherheit benötigen, da die vollständigen Entwicklungsaufzeichnungen nicht sofort verfügbar sind. Eine solche Situation kann entstehen, wenn Altsysteme gesichert werden oder wenn der Zugang zum Entwickler eingeschränkt werden kann.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

4.4.3.4 Zielsetzungen

EAL2 bietet Vertrauenswürdigkeit durch eine **vollständige** ST und durch eine Analyse der SFR in dieser ST unter Verwendung einer Funktionsspezifikation und einer Schnittstellenspezifikation, einer Leitliniendokumentation **und einer grundlegenden Beschreibung der Architektur des TOE**, um das Sicherheitsverhalten zu verstehen.

Die Analyse wird unterstützt durch eine unabhängige Prüfung der TSF, **durch einen Nachweis der Entwicklerprüfung auf Grundlage der Funktionsspezifikation, durch eine selektive unabhängige Bestätigung der Prüfungsergebnisse des Entwicklers und durch eine Anfälligkeitsanalyse (auf Grundlage der Funktionsspezifikation, des TOE-Designs, der Beschreibung der Sicherheitsarchitektur und des bereitgestellten Nachweises der Leitlinien), die die Widerstandsfähigkeit gegen eindringende Angreifer mit niedrigem Angriffspotential nachweisen.**

EAL2 bietet auch Vertrauenswürdigkeit durch den **Einsatz** eines **Konfigurationsmanagementsystems** und den **Nachweis sicherer Auslieferungsverfahren.**

Diese EAL **stellt** einen bedeutenden Zuwachs an Vertrauenswürdigkeit **gegenüber EAL1 dar, da sie Prüfungen durch den Entwickler, eine Anfälligkeitsanalyse (zusätzlich zur Suche im öffentlichen Bereich) und unabhängige Prüfungen auf der Grundlage detaillierterer TOE-Spezifikationen erfordert.**

4.4.3.5 Vertrauenswürdigkeitskomponenten

In Tabelle 3 sind die in EAL 2 enthaltenen Vertrauenswürdigkeitskomponenten aufgeführt.

Tabelle 3 — EAL2

Vertrauenswürdigkeitsklasse	Vertrauenswürdigkeitskomponenten
ADV: Entwicklung	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Leitliniendokumente	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Lebenszyklusunterstützung	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: ST-Evaluierung	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Prüfungen	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Anfälligkeitsbewertung	AVA_VAN.2 Vulnerability analysis

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

4.4.4 Vertrauenswürdigkeitsstufe 3 (EAL3) — Methodisch geprüft und kontrolliert

4.4.4.1 Paketname

Der Name des Pakets lautet „Evaluation assurance level 3“ (EAL3) — methodisch geprüft und kontrolliert.

4.4.4.2 Pakettyp

Dies ist ein Vertrauenswürdigkeitspaket.

4.4.4.3 Paketüberblick

EAL3 ermöglicht es einem gewissenhaften Entwickler, bereits in der Designphase ein Höchstmaß an Vertrauenswürdigkeit durch positive Sicherheitstechnik zu erlangen, ohne die bestehenden soliden Entwicklungspraktiken wesentlich zu verändern.

EAL3 ist in den Fällen anwendbar, in denen Entwickler oder Benutzer eine mittlere Stufe an unabhängig garantierter Sicherheit benötigen und eine gründliche Untersuchung des TOE und seiner Entwicklung ohne wesentliche Umgestaltung erforderlich ist.

4.4.4.4 Zielsetzungen

EAL3 bietet Vertrauenswürdigkeit durch eine vollständige ST und durch eine Analyse der SFR in dieser ST unter Verwendung einer Funktionsspezifikation und einer Schnittstellenspezifikation, einer Leitliniendokumentation und einer **Architekturbeschreibung** des **Designs** des TOE, um das Sicherheitsverhalten zu verstehen.

Die Analyse wird unterstützt durch unabhängige Prüfungen der TSF, durch einen Nachweis der Entwicklerprüfung auf Grundlage der Funktionsspezifikation **und des TOE-Designs**, durch eine selektive unabhängige Bestätigung der Prüfungsergebnisse des Entwicklers und durch eine Anfälligkeitsanalyse (auf Grundlage der Funktionsspezifikation, des TOE-Designs, der Beschreibung der Sicherheitsarchitektur und des bereitgestellten Nachweises der Leitlinien), die die Widerstandsfähigkeit gegen eindringende Angreifer mit niedrigem Angriffspotential nachweist.

EAL3 bietet auch Vertrauenswürdigkeit durch **den** Einsatz von **Maßnahmen für die Entwicklungsumgebung**, das Konfigurationsmanagement des **TOE** und den Nachweis sicherer Auslieferungsverfahren.

Diese EAL stellt einen bedeutenden Zuwachs an Vertrauenswürdigkeit gegenüber **EAL2** dar, da sie eine **vollständigere** Prüfungs**abdeckung** der **Sicherheits**funktionalität und der **Mechanismen und/oder Verfahren erfordert, die ein gewisses Vertrauen in die Unverfälschbarkeit des** TOE **während der Entwicklung schaffen.**

4.4.4.5 Vertrauenswürdigkeitskomponenten

In Tabelle 4 sind die in EAL 3 enthaltenen Vertrauenswürdigkeitskomponenten aufgeführt.

Tabelle 4 — EAL3

Vertrauenswürdigkeitsklasse	Vertrauenswürdigkeitskomponenten
ADV: Entwicklung	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Leitliniendokumente	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

Tabelle 4 (*fortgesetzt*)

Vertrauenswürdigkeitsklasse	Vertrauenswürdigkeitskomponenten
ALC: Lebenszyklusunterstützung	ALC_CMC.3 Authorization controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
ASE: ST-Evaluierung	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Prüfungen	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Anfälligkeitsbewertung	AVA_VAN.2 Vulnerability analysis

4.4.5 Vertrauenswürdigkeitsstufe 4 (EAL4) — Methodisch gestaltet, geprüft und bewertet

4.4.5.1 Paketname

Der Name des Pakets lautet „Evaluation assurance level 4“ (EAL4) — methodisch gestaltet, geprüft und bewertet.

4.4.5.2 Pakettyp

Dies ist ein Vertrauenswürdigkeitspaket.

4.4.5.3 Paketüberblick

EAL4 ermöglicht es einem Entwickler, ein Höchstmaß an Vertrauenswürdigkeit durch positive Sicherheitstechnik auf der Grundlage guter kommerzieller Entwicklungspraktiken zu erlangen, die zwar stringent sind, aber kein umfangreiches Fachwissen, keine Fertigkeiten und keine anderen Ressourcen erfordern. EAL4 ist die höchste Stufe, bei der eine Nachrüstung einer bestehenden Produktlinie wahrscheinlich wirtschaftlich machbar ist.

EAL4 ist daher in den Fällen anwendbar, in denen Entwickler oder Benutzer eine mittlere bis hohe Stufe unabhängig garantierter Sicherheit in herkömmlichen handelsüblichen TOE benötigen und bereit sind, zusätzliche sicherheitsspezifische Entwicklungskosten auf sich zu nehmen.

4.4.5.4 Zielsetzungen

EAL4 bietet Vertrauenswürdigkeit durch eine vollständige ST und durch eine Analyse der SFR in dieser ST unter Verwendung einer Funktionsspezifikation und einer **vollständigen** Schnittstellenspezifikation, einer

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

Leitliniendokumentation, einer Beschreibung des **grundlegenden modularen** Designs des TOE **und einer Teilmenge der Implementierung**, um das Sicherheitsverhalten zu verstehen.

Die Analyse wird unterstützt durch unabhängige Prüfungen der TSF, durch einen Nachweis der Entwicklerprüfung auf Grundlage der Funktionsspezifikation und des TOE-Designs, durch eine selektive unabhängige Bestätigung der Prüfungsergebnisse des Entwicklers und durch eine Anfälligkeitsanalyse (auf Grundlage der Funktionsspezifikation, des TOE-Designs, der **Implementierungsrepräsentation**, der Beschreibung der Sicherheitsarchitektur und des bereitgestellten Nachweises der Leitlinien), die die Widerstandsfähigkeit gegen eindringende Angreifer mit einem Angriffspotential der Stufe **Enhanced-Basic** nachweist.

EAL4 bietet auch Vertrauenswürdigkeit durch den Einsatz von Maßnahmen für die Entwicklungsumgebung **und ein zusätzliches** Konfigurationsmanagement für den TOE, **einschließlich Automatisierung** und Nachweis sicherer Auslieferungsverfahren.

Diese EAL stellt einen bedeutenden Zuwachs an Vertrauenswürdigkeit gegenüber **EAL3** dar, da sie eine umfangreichere **Beschreibung des Designs,** die **Implementierungsrepräsentation für die gesamte TSF** und **verbesserte** Mechanismen und/oder Verfahren erfordert, die Vertrauen in die Unverfälschbarkeit des TOE während der Entwicklung schaffen.

4.4.5.5 Vertrauenswürdigkeitskomponenten

In Tabelle 5 sind die in EAL 4 enthaltenen Vertrauenswürdigkeitskomponenten aufgeführt.

Tabelle 5 — EAL4

Vertrauenswürdigkeitsklasse	Vertrauenswürdigkeitskomponenten
ADV: Entwicklung	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Modular design
AGD: Leitliniendokumente	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Lebenszyklusunterstützung	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well defined developer tools
ASE: ST-Evaluierung	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12

Tabelle 5 (*fortgesetzt*)

Vertrauenswürdigkeitsklasse	Vertrauenswürdigkeitskomponenten
ATE: Prüfungen	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Anfälligkeitsbewertung	AVA_VAN.3 Focused vulnerability analysis

4.4.6 Vertrauenswürdigkeitsstufe 5 (EAL5) — Semiformal verifiziert, gestaltet und geprüft

4.4.6.1 Paketname

Der Name des Pakets lautet „Evaluation assurance level 5“ (EAL5) — semiformal gestaltet und geprüft.

4.4.6.2 Pakettyp

Dies ist ein Vertrauenswürdigkeitspaket.

4.4.6.3 Paketüberblick

EAL5 ermöglicht es einem Entwickler, ein Höchstmaß an Vertrauenswürdigkeit durch Sicherheitstechnik auf der Grundlage stringenter kommerzieller Entwicklungspraktiken zu erlangen – unterstützt durch eine moderate Anwendung spezieller Sicherheitstechniken. Ein solcher TOE wird wahrscheinlich mit der Absicht gestaltet und entwickelt, eine Vertrauenswürdigkeit nach EAL5 zu erreichen. Es ist wahrscheinlich, dass die zusätzlichen Kosten, die den EAL5-Anforderungen zuzuschreiben sind, im Vergleich zu einer stringenten Entwicklung ohne die Anwendung spezieller Techniken nicht hoch sind.

EAL5 ist daher in den Fällen anwendbar, in denen Entwickler oder Benutzer hohe unabhängig garantierte Sicherheit in einer geplanten Entwicklung benötigen und einen stringenten Entwicklungsansatz fordern, ohne dass unangemessene Kosten für spezielle Sicherheitstechniken anfallen.

4.4.6.4 Zielsetzungen

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

Die Analyse wird unterstützt durch unabhängige Prüfungen der TSF, durch einen Nachweis der Entwicklerprüfung auf Grundlage der Funktionsspezifikation und des TOE-Designs, durch eine selektive unabhängige Bestätigung der Prüfungsergebnisse des Entwicklers und **eine unabhängige** Anfälligkeitsanalyse, die die Widerstandsfähigkeit gegen eindringende Angreifer mit **einem mittleren** Angriffspotential nachweist.

EAL5 bietet auch Vertrauenswürdigkeit durch den Einsatz von Maßnahmen für die Entwicklungsumgebung und ein **umfassendes** Konfigurationsmanagement für den TOE, einschließlich Automatisierung und Nachweis sicherer Auslieferungsverfahren.

Diese EAL stellt einen bedeutenden Zuwachs an Vertrauenswürdigkeit gegenüber **EAL4** dar, da sie **semiformale Beschreibungen des Designs**, **eine** stärker **strukturierte (und damit analysierbare) Architektur** und verbesserte Mechanismen und/oder Verfahren erfordert, die das Vertrauen darin schaffen, dass der TOE während der Entwicklung nicht manipuliert werden kann.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-5:2023-12