

# E DIN EN ISO/IEC 15408-1:2024-01 (D/E)

Erscheinungsdatum: 2023-11-24

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre -  
Evaluationskriterien für IT-Sicherheit - Teil 1: Einführung und allgemeines Modell  
(ISO/IEC 15408-1:2022); Deutsche und Englische Fassung prEN ISO/IEC 15408-1:2023

Information security, cybersecurity and privacy protection - Evaluation criteria for IT  
security - Part 1: Introduction and general model (ISO/IEC 15408-1:2022); German and  
English version prEN ISO/IEC 15408-1:2023

---

Inhalt	Seite
Europäisches Vorwort.....	11
Vorwort.....	12
Einleitung.....	15
1 Anwendungsbereich.....	17
2 Normative Verweisungen.....	17
3 Begriffe.....	18
4 Symbole und Abkürzungen.....	31
5 Übersicht.....	33
5.1 Allgemein.....	33
5.2 Beschreibung der Normenreihe ISO/IEC 15408.....	33
5.2.1 Allgemein.....	33
5.2.2 Zielgruppe.....	34
5.3 Evaluierungsgegenstand (TOE).....	38
5.3.1 Allgemein.....	38
5.3.2 TOE-Grenzen.....	38
5.3.3 Unterschiedliche Darstellungen des TOEs.....	39
5.3.4 Unterschiedliche Konfigurationen des TOEs.....	39
5.3.5 Betriebsumgebung des TOE.....	40
5.4 Darstellung des Inhalts dieses Dokuments.....	40
6 Allgemeines Modell.....	41
6.1 Hintergrund.....	41
6.2 Vermögenswerte und Sicherheitsmaßnahmen.....	41
6.3 Kernkonstrukte des Paradigmas der Normenreihe ISO/IEC 15408.....	43
6.3.1 Allgemein.....	43
6.3.2 Konformitätstypen.....	44
6.3.3 Weitergabe von Sicherheitsanforderungen.....	44
6.3.4 Erfüllung der Bedürfnisse der Verbraucher (Risikoeigentümer).....	48
7 Festlegung von Sicherheitsanforderungen.....	49
7.1 Sicherheitsproblemdefinition (SPD).....	49
7.1.1 Allgemein.....	49
7.1.2 Bedrohungen.....	50
7.1.3 Organisatorische Sicherheitsrichtlinien (OSP).....	50
7.1.4 Annahmen.....	51
7.2 Sicherheitszielsetzungen.....	52
7.2.1 Allgemein.....	52
7.2.2 Sicherheitszielsetzungen für den TOE.....	52
7.2.3 Sicherheitszielsetzungen für die Betriebsumgebung.....	52

7.2.4	Beziehung zwischen Sicherheitszielsetzungen und der SPD .....	53
7.2.5	Rückverfolgung zwischen Sicherheitszielsetzungen und der SPD.....	53
7.2.6	Bereitstellen einer Begründung für die Rückverfolgung .....	54
7.2.7	Zum Entgegenwirken von Bedrohungen .....	54
7.2.8	Sicherheitszielsetzungen: Schlussfolgerung .....	55
7.3	Sicherheitsanforderungen .....	55
7.3.1	Allgemein.....	55
7.3.2	Sicherheitsfunktionsanforderungen (SFR).....	56
7.3.3	Vertrauenswürdigkeitsanforderungen (SARs) .....	58
7.3.4	Sicherheitsanforderungen: Schlussfolgerung.....	59
8	Sicherheitskomponenten .....	60
8.1	Hierarchische Struktur der Sicherheitskomponenten .....	60
8.1.1	Allgemein .....	60
8.1.2	Klasse .....	61
8.1.3	Familie .....	61
8.1.4	Komponente.....	61
8.1.5	Element.....	61
8.2	Operationen .....	61
8.2.1	Allgemein .....	61
8.2.2	Iteration .....	62
8.2.3	Zuweisung.....	63
8.2.4	Auswahl .....	64
8.2.5	Präzisierung.....	65
8.3	Abhängigkeiten zwischen Komponenten .....	67
8.4	Erweiterte Komponenten .....	68
8.4.1	Allgemein .....	68
8.4.2	Definieren erweiterter Komponenten .....	68
9	Pakete .....	69
9.1	Allgemein .....	69
9.2	Pakettypen .....	69
9.2.1	Allgemein .....	69
9.2.2	Vertrauenswürdigkeitspakete.....	70
9.2.3	Funktionspakete.....	70
9.3	Paketabhängigkeiten .....	71
9.4	Evaluierungsmethode(n) und -aufgaben.....	71
10	Schutzprofile (PP) .....	71
10.1	Allgemein .....	71
10.2	PP-Einleitung.....	72
10.3	Konformitätsansprüche und Konformitätserklärungen.....	72
10.4	Vertrauenswürdigkeitsanforderungen (SARs) .....	75
10.5	Zusätzliche gemeinsame Anforderungen an die strikte und nachweisliche Konformität .....	75
10.5.1	Konformitätsansprüche und Konformitätserklärungen.....	75
10.5.2	Sicherheitsproblemdefinition (SPD) .....	76
10.5.3	Sicherheitszielsetzungen.....	76
10.6	Zusätzliche Anforderungen speziell für die strikte Konformität .....	76
10.6.1	Anforderungen an die Sicherheitsproblemdefinition (SPD) .....	76
10.6.2	Anforderungen an die Sicherheitszielsetzungen .....	76
10.6.3	Anforderungen an die Sicherheitsanforderungen .....	77
10.7	Zusätzliche Anforderungen speziell für die nachweisliche Konformität.....	77
10.8	Zusätzliche Anforderungen speziell für die genaue Konformität .....	77
10.8.1	Allgemein.....	77
10.8.2	Konformitätsansprüche und -erklärungen .....	78
10.9	Unter Verwendung von PP .....	78
10.10	Konformitätserklärungen und -ansprüche im Falle mehrerer PP.....	79
10.10.1	Allgemein.....	79
10.10.2	Wenn strikte oder nachweisliche Konformität festgelegt ist .....	79

10.10.3	Wenn genaue Konformität festgelegt ist .....	79
11	Modularer Aufbau der Anforderungen .....	79
11.1	Allgemein .....	79
11.2	PP-Module.....	80
11.2.1	Allgemein .....	80
11.2.2	PP-Modulbasis.....	80
11.2.3	Anforderungen an PP-Module.....	80
11.3	PP-Konfigurationen .....	84
11.3.1	Allgemein .....	84
11.3.2	Anforderungen an PP-Konfigurationen .....	85
11.3.3	Verwendung von PP-Konfigurationen.....	91
12	Sicherheitsvorgaben (ST) .....	94
12.1	Allgemein .....	94
12.2	Konformitätsansprüche und -erklärungen.....	95
12.3	Vertrauenswürdigkeitsanforderungen.....	97
12.4	Zusätzliche Anforderungen im Fall der genauen Konformität.....	98
12.4.1	Zusätzliche Anforderungen für den Konformitätsanspruch.....	98
12.4.2	Zusätzliche Anforderungen für die SPD .....	98
12.4.3	Zusätzliche Anforderungen an die Sicherheitszielsetzungen.....	98
12.4.4	Zusätzliche Anforderungen an die Sicherheitsanforderungen .....	99
12.5	Zusätzliche Anforderungen im Fall der Mehrfach-Vertrauenswürdigkeit.....	99
13	Evaluierung und Evaluierungsergebnisse.....	101
13.1	Allgemein .....	101
13.2	Evaluierungskontext .....	103
13.3	Evaluierung der PP und PP-Konfigurationen.....	104
13.4	Evaluierung von ST .....	105
13.5	Evaluierung von TOE.....	105
13.6	Evaluierungsmethoden und Evaluierungsaufgaben .....	106
13.7	Evaluierungsergebnisse.....	106
13.7.1	Ergebnisse einer PP-Evaluierung.....	106
13.7.2	Ergebnisse der Evaluierung einer PP-Konfiguration.....	106
13.7.3	Ergebnisse einer ST-/TOE-Evaluierung .....	106
13.8	Evaluierung mit Mehrfach-Vertrauenswürdigkeit.....	107
14	Zusammensetzung der Vertrauenswürdigkeit.....	108
14.1	Allgemein .....	108
14.2	Zusammensetzungsmodelle .....	109
14.2.1	Mehrschichtiges Zusammensetzungsmodell.....	109
14.2.2	Netzwerk- oder bi-direktionales Zusammensetzungsmodell.....	110
14.2.3	Eingebettetes Zusammensetzungsmodell.....	111
14.3	Evaluierungstechniken für die Vertrauenswürdigkeit von Zusammensetzungsmodellen ....	112
14.3.1	Allgemein .....	112
14.3.2	ACO-Klasse für zusammengesetzte TOE .....	112
14.3.3	Verbundevaluation für Verbundprodukte.....	113
14.4	Anforderungen an Evaluierungen, die Zusammensetzungstechniken verwenden.....	126
14.4.1	Wiederverwendung von Evaluierungsergebnissen .....	126
14.4.2	Aspekte der zusammengesetzten Evaluierung.....	126
14.5	Evaluierung mittels Zusammensetzung und Mehrfach-Vertrauenswürdigkeit .....	128
Anhang A (normativ)	Spezifikation von Paketen .....	129
A.1	Ziel und Aufbau dieses Anhangs.....	129
A.2	Paketfamilien .....	129
A.2.1	Allgemein .....	129
A.2.2	Name der Paketfamilie .....	129
A.2.3	Überblick über die Paketfamilie .....	129
A.2.4	Zielsetzungen der Paketfamilie .....	129
A.2.5	Pakete.....	129

A.3	Pakete .....	129
A.3.1	Verpflichtender Inhalt eines Pakets .....	129
A.3.2	Optionalen Inhalt eines Pakets .....	131
<b>Anhang B (normativ) Spezifikation von Schutzprofilen (PP) .....</b>		<b>133</b>
B.1	Ziel und Aufbau dieses Anhangs .....	133
B.2	Spezifikation eines PP .....	133
B.2.1	Wie ein PP verwendet werden sollte .....	133
B.2.2	Wie ein PP nicht verwendet werden sollte .....	134
B.3	Verpflichtender Inhalt eines PPs .....	134
B.3.1	Allgemein .....	134
B.3.2	PP-Einleitung (APE_INT) .....	136
B.3.3	Konformitätsansprüche und Konformitätserklärung (APE_CCL) .....	138
B.3.4	Sicherheitsproblemdefinition (SPD) (APE_SPD) .....	139
B.3.5	Sicherheitszielsetzungen (APE_OBJ) .....	139
B.3.6	Erweiterte Komponentendefinition (APE_ECD) .....	139
B.3.7	Sicherheitsanforderungen (APE_REQ) .....	140
B.4	Verweisen auf andere Normen in einem PP .....	140
B.5	Die PP mit direkter Begründung .....	141
B.5.1	Allgemein .....	141
B.5.2	Konformitätsansprüche (APE_CCL) für die PP mit direkter Begründung .....	142
B.5.3	Sicherheitszielsetzungen (APE_OBJ) für PP mit direkter Begründung .....	143
B.6	Optionalen Inhalt eines PP .....	143
<b>Anhang C (normativ) Spezifikation von PP-Modulen und PP-Konfigurationen .....</b>		<b>144</b>
C.1	Ziel und Aufbau dieses Anhangs .....	144
C.2	Spezifikation von PP-Modulen .....	144
C.2.1	Unter Verwendung eines PP-Moduls .....	144
C.2.2	Verpflichtender Inhalt eines PP-Moduls .....	144
C.2.3	PP-Module mit direkter Begründung .....	151
C.2.4	Leitlinien für die Einbeziehung von SPD-Elementen aus einer PP-Modulbasis .....	152
C.2.5	Optionalen Inhalt eines PP-Moduls .....	153
C.3	Spezifikation von PP-Konfigurationen .....	153
C.3.1	Allgemein .....	153
C.3.2	PP-Konfigurationsverweisung .....	154
C.3.3	Komponentenerklärung .....	154
C.3.4	TOE-Überblick .....	155
C.3.5	Konsistenzbegründung .....	155
C.3.6	Konformitätsanspruch und Konformitätserklärung .....	155
C.3.7	SAR-Aussage .....	157
<b>Anhang D (normativ) Spezifikation von Sicherheitsvorgaben (ST) und ST mit direkter Begründung .....</b>		<b>158</b>
D.1	Ziel und Aufbau dieses Anhangs .....	158
D.2	Verwendung einer ST .....	158
D.2.1	Wie eine ST verwendet werden sollte .....	158
D.2.2	Wie eine ST nicht verwendet werden sollte .....	159
D.2.3	Fragen, die mit einer ST beantwortet werden können .....	159
D.3	Verpflichtender Inhalt einer ST .....	160
D.3.1	Allgemein .....	160
D.3.2	ST-Einleitung (ASE_INT) .....	162
D.3.3	Konformitätsansprüche (ASE_CCL) .....	165
D.3.4	Sicherheitsproblemdefinition (SPD) (ASE_SPD) .....	165
D.3.5	Sicherheitszielsetzungen (ASE_OBJ) .....	165
D.3.6	Erweiterte Komponentendefinition (ASE_ECD) .....	165
D.3.7	Sicherheitsanforderungen (ASE_REQ) .....	166
D.3.8	Zusammenfassende Spezifikation des TOEs (ASE_TSS) .....	167
D.4	ST mit direkter Begründung .....	168
D.4.1	Allgemein .....	168

D.4.2	Konformitätsansprüche (ASE_CCL) für ST mit direkter Begründung.....	169
D.4.3	Sicherheitsproblemdefinition (SPD) (ASE_SPD) für ST mit direkter Begründung .....	170
D.4.4	Sicherheitsanforderungen (ASE_REQ) für ST mit direkter Begründung.....	170
D.5	Verweisen auf andere Normen in einer ST .....	170
<b>Anhang E (normativ) Konformität des/der PP/PP-Konfiguration .....</b>		<b>171</b>
E.1	Allgemein .....	171
E.2	Nachweisliche Konformität.....	172
E.3	Strikte Konformität .....	172
E.4	Genau Konformität .....	172
E.4.1	Allgemein .....	172
E.4.2	FAQ/Cheatsheet zu genauer Konformität .....	175
Literaturhinweise .....		177
<b>Bilder</b>		
Bild 1 — Sicherheitskonzepte und Beziehungen.....		42
Bild 2 — Evaluierungskonzepte und Beziehungen .....		43
Bild 3 — Rückverfolgungen zwischen Sicherheitszielsetzungen und der SPD .....		54
Bild 4 — Beziehungen zwischen SPD, Sicherheitszielsetzungen und Sicherheitsanforderungen.....		60
Bild 5 — Beispiel einer PP-Konfiguration.....		91
Bild 6 — Verwendung von PP-Konfigurationen mit Einfach- und Mehrfach- Vertrauenswürdigkeit.....		92
Bild 7 — Zusammensetzung von PP-Komponenten .....		93
Bild 8 — Vertrauenswürdigkeitsklassen, die zur Evaluierung der PP, PP-Konfigurationen und ST verwendet werden .....		94
Bild 9 — Beispiel einer ST mit Mehrfach-Vertrauenswürdigkeit.....		101
Bild 10 — Ablauf der Evaluierung .....		102
Bild 11 — Mehrschichtiges Zusammensetzungsmodell.....		109
Bild 12 — Netzwerk- oder bi-direktionales Zusammensetzungsmodell.....		110
Bild 13 — Eingebettetes Zusammensetzungsmodell .....		111
Bild 14 — Unter Verwendung der ACO-Klasse evaluierter zusammengesetzter TOE.....		112
Bild 15 — Verbundevaluation.....		115
Bild A.1 — Aufbau einer Paketfamilie mit Vertrauenswürdigkeits- oder Funktionspaketen .....		130
Bild B.1 — Inhalt eines Schutzprofils .....		135
Bild B.2 — Inhalt eines PP mit direkter Begründung.....		142
Bild C.1 — Inhalt eines PP-Moduls .....		145

<b>Bild C.2 — Übernommene Konformitätsansprüche und -erklärungen für den Fall der genauen Konformität.....</b>	<b>149</b>
<b>Bild C.3 — Inhalte eines PP-Moduls mit direkter Begründung.....</b>	<b>152</b>
<b>Bild C.4 — Inhalt einer PP-Konfiguration .....</b>	<b>154</b>
<b>Bild C.5 — PP-Konfiguration und genaue Konformität .....</b>	<b>157</b>
<b>Bild D.1 — Inhalt einer ST .....</b>	<b>161</b>
<b>Bild D.2 — Inhalt einer ST mit direkter Begründung.....</b>	<b>169</b>
<b>Bild E.1 — Genaue Konformität einer ST mit mehreren PP .....</b>	<b>174</b>
<b>Bild E.2 — Genaue Konformität mit einer PP-Konfiguration mit mehreren PP und PP-Modulen .....</b>	<b>175</b>
<b>Tabellen</b>	
<b>Tabelle 1 — Roadmap für die „Evaluierungskriterien für IT-Sicherheit“ .....</b>	<b>36</b>
<b>Tabelle 2 — Informationen, die dem Entwickler der abhängigen Komponente zur Verfügung zu stellen sind.....</b>	<b>117</b>
<b>Tabelle 3 — Informationen, die dem Evaluator für Verbundprodukte und der Evaluierungsinstanz für Verbundprodukte zur Verfügung zu stellen sind.....</b>	<b>118</b>
<b>Tabelle E.1 — Zusammenfassung der genauen Konformität.....</b>	<b>175</b>