

# DIN EN ISO/IEC 15408-1:2020-12 (D)

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

---

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