

Kai Rannenberg

Zertifizierung mehrseitiger IT-Sicherheit

**Kriterien und organisatorische
Rahmenbedingungen**



Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Rannenberg, Kai:

Zertifizierung mehrseitiger IT-Sicherheit: Kriterien und
organisatorische Rahmenbedingungen / Kai Rannenberg. –

Braunschweig; Wiesbaden: Vieweg, 1998

(DuD-Fachbeiträge)

ISBN 978-3-528-05666-7

ISBN 978-3-322-90281-8 (eBook)

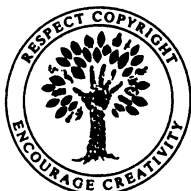
DOI 10.1007/978-3-322-90281-8

Alle Rechte vorbehalten

© Springer Fachmedien Wiesbaden 1998

Ursprünglich erschienen bei Friedr. Vieweg & Sohn Verlagsgesellschaft mbH,
Braunschweig/Wiesbaden 1998

Der Verlag Vieweg ist ein Unternehmen der Bertelsmann Fachinformation GmbH.



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

<http://www.vieweg.de>

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, daß solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Verbreitung unserer Werke wollen wir die Umwelt schonen: Dieses Werk ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei Verbrennung Schadstoffe freisetzen.

Gesamtherstellung: Lengericher Handelsdruckerei, Lengerich

ISBN 978-3-528-05666-7

Inhaltsübersicht

Inhaltsübersicht	V
Vorwort.....	VII
Inhaltsverzeichnis	XIII
Abbildungsverzeichnis	XIX
Teil A: IT-Sicherheitszertifizierung und mehrseitige IT-Sicherheit.....	1
1 Zertifizierung, Kriterien und ihre Rahmenbedingungen	3
2 Mehrseitige IT-Sicherheit, Kriterien und Zertifizierung.....	19
Teil B: Die etablierten Kriterien und die Erfahrungen mit ihnen	29
3 Die Trusted Computer System Evaluation Criteria (TCSEC).....	31
4 Die europäischen ITSEC und die deutschen ZSISC	41
5 Bewertung der etablierten Zertifizierungs- und Kriterienszenarie	65
Teil C: Die Post-ITSEC-Kriterien	73
6 Die kanadischen CTCPEC.....	75
7 Die ISO/IEC-ECITS.....	79
8 Die Common Criteria	87
9 Die Post-ITSEC-Kriterien im Lichte der ITSEC-Kritik	97
Teil D: Konzepte für Kriterien für mehrseitig sichere Systeme.....	105
10 Eine neue Gliederung von Sicherheitsfunktionalität	107
11 Eine Funktionalitätsklasse für TK-Anlagen als Beispiel	121
Teil E: Organisation der Zertifizierung und der Weiterentwicklung ihrer fachlichen Grundlagen.....	135
12 Aufgaben der Organisation.....	137
13 Zertifizierung.....	157
14 Evaluation	169
15 Akkreditierung der Evaluationsstellen	175
16 Information und Beratung der Nicht-Insider.....	181
17 Weiterentwicklung von Kriterien und Methoden.....	185
Nachwort	193
Anhänge.....	195
Anhang A: Literatur.....	197
Anhang B: TK-Funktionalitätsklasse nach ITSEC.....	215
Anhang C: Stichwortverzeichnis	221
Anhang D: Abkürzungsverzeichnis	227

Vorwort

Telekommunikation wird nicht nur immer wichtiger für Arbeitswelt und Privatleben, sie basiert auch in zunehmendem Maße auf Informationstechnik (IT). Der Austausch von Bestell-, Produktions- und Konstruktionsdaten zwischen Unternehmen ist ein Beispiel dafür, ebenso die Internet-Recherche von Privatpersonen. Selbst der schon „klassisch“ anmutende Telefonanruf „von Mensch zu Mensch“ wird durch Rechner technisch gestützt und vermittelt. Die Gesellschaft ist, wie auf begeh- und befahrbare Straßen, auf eine funktionsfähige Telekommunikationsinfrastruktur angewiesen, und niemand kann sich ihr wirklich entziehen.

Damit ergeben sich Anforderungen an die Sicherheit dieser Telekommunikation und der ihr zugrundeliegenden Informationstechnik, die sich unter dem Begriff „Mehrseitige Sicherheit“ zusammenfassen lassen. Mehrseitige Sicherheit bedeutet, daß nicht nur die Sicherheit einer der an der Kommunikation beteiligten Parteien berücksichtigt wird. Dies gilt für Diensteanbieter, Netzbetreiber, aber auch für Teilnehmer oder Nutzer. Wichtig sind insbesondere der Schutz und die Stärkung der Teilnehmer und Nutzer, damit ernsthafte – etwa kommerzielle – Anwendungen überhaupt realisierbar sind. Wer einerseits keine Kontrolle über seine via Homebanking verwalteten Finanzen oder seine elektronische Unterschrift hat und andererseits fürchten muß, daß sein Einkaufs- oder Telefonverhalten von anderen kontrolliert und ausgewertet werden kann, wird kein Vertrauen in die Technik fassen, sondern sich bei ihrer Nutzung und der damit verknüpften Übernahme von Verantwortung und Preisgabe persönlicher Informationen eher zurückhalten. Dies gilt erst recht, da elektronisch erfaßte Information als immaterielles Gut mindestens eine besondere Eigenschaft hat: Sie läßt sich zwar vergleichsweise leicht sammeln, nutzen und vervielfältigen, jedoch kann kaum eine Garantie für ihre Vernichtung oder Löschung gegeben werden, insbesondere nicht angesichts weltweiter Computernetze.

Wichtig für Vertrauen ist nicht nur, daß mehrseitige Sicherheit technisch unterstützt wird, sondern auch, daß sie als Eigenschaft der jeweiligen Kommunikations- oder Informationstechnik *erkennbar* ist. Diese Anforderung kollidiert mit der Komplexität heutiger Hardware- und Softwarekomponenten und erst recht der Komplexität zusammengesetzter Systeme, deren Sicherheitseigenschaften nicht durch einfache „Draufschau“, sondern nur durch sorgfältige Prüfung zu ermitteln sind.

Ein seit den 70er Jahren beschrittener Weg, begründetes Vertrauen in Informationstechnik zu schaffen, ist die Evaluation und Zertifizierung der entsprechenden Produkte auf der Basis veröffentlichter Kriterien, sogenannter IT-Sicherheitsevaluationskriterien. Zertifikate mit Aussagen über

Sicherheitseigenschaften sollen Anwendern helfen, die angebotenen Produkte bezüglich ihrer Sicherheit zu beurteilen und auch untereinander zu vergleichen. Vergeben werden die Zertifikate von möglichst unabhängigen und fachkundigen Stellen. Als Voraussetzung muß das jeweilige Produkt eine Evaluation durch eine neutrale Instanz, im allgemeinen ein Prüflabor, erfolgreich bestehen. Entsprechende Zertifizierungssysteme existieren schon seit einiger Zeit in mehreren Staaten.

Grundlage der Evaluationen sind Kriterienkataloge wie die im Rahmen der Europäischen Gemeinschaft harmonisierten „Information Technology Security Evaluation Criteria“ (ITSEC). Es ist absehbar, daß diese Kriterien erheblichen Einfluß auf die Entwicklung von IT-Systemen haben werden, da z.B. verschiedene Anwender der öffentlichen Hand Zertifikate zur Voraussetzung für die Zulassung von Produkten machen wollen. Anwenderorganisationen, wie etwa die Kassenärztliche Bundesvereinigung, haben dies bereits getan. Zusätzlich enthalten Gesetz und Verordnung zur digitalen Signatur eine entsprechende Vorschrift für wesentliche technische Komponenten, etwa zum Signieren und zum Schlüsselmanagement.

Die bisher gültigen Kriterienkataloge haben jedoch nach Ansicht vieler Kritiker erhebliche Schwächen und Lücken, gerade wenn es darum geht, im Hinblick auf mehrseitige Sicherheit zu evaluieren. Diese Schwächen wirken sich besonders bei der Anwendung auf rechnergestützte Kommunikationstechnik aus. Sie sind neben Problemen der weltweiten Harmonisierung ein Grund dafür, daß auch in der internationalen Normung (z.B. bei ISO/IEC) an Evaluationskriterien gearbeitet wird.

Ziele und Gliederung dieses Buches

In den fünf Teilen dieses Buches werden Evaluationskriterien, Zertifizierungssysteme und die relevanten Rahmenbedingungen im Hinblick auf die Anforderungen mehrseitiger Sicherheit untersucht und Verbesserungen vorgeschlagen. Drei Ziele werden dabei vorrangig verfolgt:

- (1) Kriterien und Maßstäbe sollen mehrseitige Sicherheit als Qualitätsmerkmal erkennbar, prüfbar und zertifizierbar machen.
- (2) Zertifizierung, Evaluation und die Information darüber sollen Anwendern und Nutzern eine realistische Möglichkeit geben, das für sie Relevante zu erfahren, den jeweiligen Zertifikaten in angemessenem Umfang zu vertrauen und um deren Grenzen zu wissen.
- (3) Die Organisation der Zertifizierung und der Weiterentwicklung der Kriterien sollen auch auf neue oder heute noch unbekannte Anforderungen reagieren können.

Die zur Bearbeitung nötige Zusammenführung technischer und organisatorischer Argumente verlangt einen ständigen Spagat zwischen unterschiedlichen Gebieten. Einige Zusammenhänge zwischen Politik und technischer Entwicklung – oder Nichtentwicklung – ließen sich erst während jahrelanger Mitarbeit in der Normung ermitteln bzw. erfahren. Zudem ist Sicherheit mindestens innerhalb der Informationstechnik ein Querschnittsgebiet, was den Untersuchungsraum noch weiter aufspannt und die Lektüre nicht immer vereinfacht. Dies und die Tatsache, daß zum Thema „IT-

Sicherheitszertifizierung und -kriterien“ Überblicksliteratur fehlt, machten eine recht umfangreiche Darstellung des Standes von Praxis und Entwicklung erforderlich. Deswegen führt **Teil A** zunächst allgemein in IT-Sicherheitszertifizierung und -kriterien sowie das Konzept „Mehrseitige IT-Sicherheit“ ein.

In Kapitel 1 werden Zertifizierungsorganisationen und kurz die entsprechenden Kriterien vorgestellt, zum einen allgemein, zum anderen aus Sicht der beteiligten Parteien (Hersteller und Verkäufer, Anwender und Beschaffer, Evaluations- und Zertifizierungsstellen). Beschrieben wird auch das – nicht per se konfliktfreie – Verhältnis und Zusammenspiel dieser Instanzen. Der Schwerpunkt der Darstellung liegt auf der deutschen Zertifizierungslandschaft, jedoch werden auch die Zertifizierungssysteme anderer Staaten (etwa Großbritanniens und der USA) betrachtet, insbesondere wenn die Situation dort sich strukturell von der deutschen unterscheidet. Am Ende des Kapitels steht eine Übersicht der nationalen und internationalen Initiativen zur Erstellung und Harmonisierung von IT-Sicherheitskriterien, die gegenwärtig eng mit den jeweiligen Zertifizierungssystemen verknüpft sind. Traditionell spiegeln die Evaluationskriterien auch das Verständnis, das ihre Autoren von IT-Sicherheit haben, wider. Kapitel 2 beschreibt deshalb die Entwicklung im Verständnis von IT-Sicherheit und stellt „Mehrseitige IT-Sicherheit“ früheren Ansätzen gegenüber.

In **Teil B** werden die wichtigsten bislang etablierten Kriterienkataloge vorgestellt und bewertet, um eine Einschätzung des Standes der Praxis, insbesondere bezüglich mehrseitiger IT-Sicherheit, zu geben. Im einzelnen werden in Kapitel 3 die US-amerikanischen „Trusted Computer System Evaluation Criteria“ vorgestellt, in Kapitel 4 die europäischen ITSEC und ihre prägenden deutschen Vorläufer „IT-Sicherheitskriterien“. Erfahrungen mit diesen Kriterien münden in eine zusammenfassende Bewertung der gegenwärtig etablierten Zertifizierungs- und Kriterienlandschaft (Kapitel 5) und speziell der ITSEC als der gegenwärtig in Europa gültigen Kriterien.

Die Schwächen der ITSEC sowie handelspolitische Motive veranlaßten die Entwicklung weiterer Kriterien bzw. Kriterienentwürfe. **Teil C** ist diesen „Post-ITSEC-Kriterien“ und damit dem Stand der Entwicklung gewidmet. Beschrieben werden die jüngste Version der „Canadian Trusted Computer Product Evaluation Criteria“ (Kapitel 6), die in der Normung bei ISO/IEC entstandenen Entwürfe (Kapitel 7) sowie die sogenannten „Common Criteria“, die von Regierungsbehörden sechser Atlantikanrainerstaaten erstellt wurden (Kapitel 8). In Kapitel 9 werden diese Post-ITSEC-Kriterien der Kritik an ihren Vorgängern gegenübergestellt, um den Stand der Entwicklung zu dokumentieren.

Auch die Post-ITSEC-Kriterien weisen, gemessen an den Anforderungen mehrseitiger Sicherheit, noch erhebliche Schwächen auf. Deswegen werden in den Teilen D und E Verbesserungsvorschläge zu Kriterien und zur Zertifizierungsorganisation diskutiert.

Teil D enthält Konzepte für Kriterien mehrseitig sicherer IT-Systeme, speziell in Kapitel 10 eine neue Gliederung für Sicherheitsfunktionalität, die datensparsame Verfahren zum Nutzer- und Datenschutz berücksichtigt. Diese Gliederung wird als Beleg ihrer Tauglichkeit und ihres Verbesse-

rungspotentials auf das Beispiel einer ursprünglich an den ITSEC orientierten Funktionalitätsklasse für Telekommunikationsanlagen angewandt (Kapitel 11).

Auch neue und bessere Kriterien können jedoch allein aus sich heraus nicht alle Probleme der Zertifizierungs- und Kriterienlandschaft beseitigen. Dies gilt etwa für die vielfach als unzureichend angesehene Aussagekraft und Verwertbarkeit der Ergebnisse, für die als zu hoch beklagten Kosten sowie besonders für die als zu gering erachtete Effizienz des Evaluations- und Zertifizierungsprozesses. Um diese Probleme einer Lösung zumindest näher zu bringen, sind auch Verbesserungen der Organisation der Zertifizierung und ihrer Teilaufgaben sowie der Weiterentwicklung der fachlichen Grundlagen nötig. Vorschläge dafür enthält **Teil E**.

Zunächst werden in Kapitel 12 die Teilaufgaben der Organisation und die Anforderungen an die beteiligten Instanzen zusammengetragen und systematisiert. In den Kapiteln 13 bis 17 werden dann für jede Teilaufgabe die bestehenden Organisationsformen an den Anforderungen gemessen und mit Vorschlägen für neue Organisationsformen verglichen. Zertifizierung ist dabei Gegenstand des Kapitels 13, Evaluation des Kapitels 14. Kapitel 15 ist der Akkreditierung von Evaluationsstellen gewidmet, Kapitel 16 der Information und Beratung der Nicht-Insider. In Kapitel 17 werden Organisationsformen zur Weiterentwicklung von Evaluationskriterien und Methoden diskutiert.

Die auf den ersten Blick eher kriterienfernen Aufgaben wie Zertifizierung und Akkreditierung werden u.a. deswegen ausführlich berücksichtigt, weil die Aufgaben und die beteiligten Akteure oft so eng miteinander verflochten sind, daß die Verteilung von Kompetenz bei einer Aufgabe (etwa der Akkreditierung von Prüflabors) sich auf die Arbeiten an einer anderen Aufgabe (etwa der Weiterentwicklung der Kriterien) auswirken kann. Diese Verflechtungen und mögliche Konsequenzen daraus werden auf diese Weise mit dokumentiert und berücksichtigt.

Danksagung

Ein Text dieser Art und das zugrundeliegende Projekt waren nicht möglich ohne die Unterstützung vieler Beteiligter, auch wenn sie nicht alle namentlich erwähnt werden können. Grundlage dieses Buches ist meine Dissertation an der Albert-Ludwigs-Universität Freiburg, für die sich Prof. Dr. Günter Müller als Doktorvater und Erstgutachter zur Verfügung gestellt hat. Ihm gebührt Dank nicht nur für viele Hinweise und Hilfen, sondern auch dafür, daß er sich zu einer Zeit auf ein Thema eingelassen hat, als dessen Bedeutung nicht überall so klar war wie heute. Prof. Dr. Hans-Hermann Francke hat nicht nur das Zweitgutachten übernommen, sondern mit seinem Interesse an Arbeit und Doktorand sowie beider Fortschritt eben dazu sehr beigetragen. Der Gottlieb Daimler- und Karl Benz-Stiftung, Ladenburg verdanke ich die nicht nur materielle Unterstützung meiner Arbeit im Rahmen des Kollegs „Sicherheit in der Kommunikationstechnik“.

Obwohl nicht formell beteiligt, hat Prof. Dr. Andreas Pfitzmann wesentlich bei Themenfindung und -fokussierung geholfen und neben vielem anderem geduldig frühe Versionen vieler Kapitel und Ansätze begutachtet und diskutiert. Außerdem hat er wie Rüdiger Dierstein und Prof. Dr. Fritz

Krückeberg nicht nur immer wieder inhaltlich Anteil genommen, sondern auch in bewegten Zeiten Ansatz und Idee der Arbeit im und mit dem Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit“ der Gesellschaft für Informatik stark und mutig gefördert.

Dr. Klaus-Jürgen Eckardt erklärte mir nach einer sehr lebendigen Podiumsdiskussion auf der VIS'91, wenn ich zum Thema Kriterien wirklich etwas bewegen wolle, müsse ich in die Normung gehen – wohl einer der folgenreichsten Ratschläge, die ich je bekam. Manche Erkenntnisse und Einsichten wären ohne die offenen Worte vieler Aktiver bei ISO/IEC JTC1/SC27 und DIN NI-27 schwerer oder unmöglich zu erlangen gewesen. Es sind zu viele Personen, um sie hier einzeln aufzuführen, aber ich weiß auch, daß das mindestens einigen angesichts der Materie sehr recht ist. Auch manche Diskussion im nationalen Arbeitskreis „IT-Sicherheitskriterien“ hat zur Schärfung des Problemverständnisses beigetragen.

Dankbar bin ich auch meinen Kollegen in der Abteilung Telematik des Instituts für Informatik und Gesellschaft der Universität Freiburg, speziell Dr. Werner Langenheder, der leider die Vollendung dieser Arbeit nicht mehr erleben konnte, obwohl er sehr dazu beigetragen hat. Dr. Ulrich Kohl, Dr. Frank Stoll und Dr. Marjan Jurecic haben mich freundlich in der „Sicherheitsgruppe“ aufgenommen. Ohne die Rückendeckung und Rücksicht bei vielen Projektarbeiten, die fruchtbaren Diskussionsbeiträge sowie das geduldige Korrekturlesen von Herbert Damker, Martin Reichenbach und Sönke Gold wären wohl weder Dissertation noch Buch je fertig geworden. Uwe Jendricke hat noch kurz vor Toreschluß die (vor-)letzten Tipp- und Satzfehler sowie spezielle Gemeinheiten der Textverarbeitung aufgespürt. Vielen weiteren Kollegen, speziell Dr. Tim Bussiek und Boris Padovan, danke ich für hilfreiche Einführungen und Exkurse in die Volkswirtschaft.

Last but not least ist denen zu danken, die mit dafür sorgten, daß aus der Dissertation ein Buch wurde: den vier Herausgebern der DuD-Fachbeiträge sowie Dr. Ulrike Walter und Dr. Reinald Klockenbusch vom Verlag Vieweg, die Projekt und Autor zielorientiert und einfühlsam betreuten.

Inhaltsverzeichnis

Inhaltsübersicht	V
Vorwort.....	VII
Inhaltsverzeichnis	XIII
Abbildungsverzeichnis	XIX
Teil A: IT-Sicherheitszertifizierung und mehrseitige IT-Sicherheit.....	1
1 Zertifizierung, Kriterien und ihre Rahmenbedingungen	3
1.1 Warum Zertifizierung und Evaluation nach Kriterien?	3
1.2 „Evaluation“, „Zertifizierung“ und „Akkreditierung“	4
1.3 Was wird evaluiert und zertifiziert?	5
1.4 Wie wird evaluiert, zertifiziert und akkreditiert?	6
1.5 Wer evaluiert, zertifiziert und akkreditiert?	8
1.5.1 Institutionen in Deutschland	9
1.5.2 Institutionen in anderen europäischen Staaten.....	11
1.5.3 Institutionen in den USA	12
1.5.4 Institutionen in Kanada	13
1.5.5 Institutionen in Australien	13
1.6 Wer nutzt Zertifikate und Kriterien wozu?	13
1.6.1 Nutzen für Hersteller und Verkäufer	14
1.6.2 Nutzen für Anwender und Beschaffer	15
1.6.3 Nutzen für Evaluations- und Zertifizierungsstellen.....	16
1.7 Wer schreibt welche Kriterien?.....	16
2 Mehrseitige IT-Sicherheit, Kriterien und Zertifizierung.....	19
2.1 Bedrohungen, Schutzziele und Schutzgüter.....	19
2.2 Potentielle Angreifer	21
2.3 Mehrseitige Sicherheit	24
2.4 Realisierung mehrseitiger Sicherheit in verteilten Systemen	25
2.5 Anforderungen an Kriterien und Zertifizierung.....	26
Teil B: Die etablierten Kriterien und die Erfahrungen mit ihnen	29
3 Die Trusted Computer System Evaluation Criteria (TCSEC).....	31
3.1 Konzepte der TCSEC.....	31
3.1.1 Referenzmonitor und Referenzvalidierungsmechanismus	32
3.1.2 Formale Sicherheitspolitikmodelle und das Bell-LaPadula-Modell	33
3.1.3 Die „Trusted Computing Base“	33
3.1.4 Die Kontrollzielsetzungen	34

3.2	Die Levels der TCSEC.....	35
3.2.1	Gruppe D: Minimaler Schutz.....	35
3.2.2	Gruppe C: Benutzerbestimbarer Schutz.....	35
3.2.2.1	Level C1: Benutzerbestimbarer Geheimschutz.....	36
3.2.2.2	Level C2: Schutz durch Zugriffskontrolle	36
3.2.3	Gruppe B: Vorgeschriebener Schutz	36
3.2.3.1	Level B1: Schutz durch Kennzeichnung	36
3.2.3.2	Level B2: Schutz durch Strukturierung.....	36
3.2.3.3	Level B3: Sicherheitsdomänen	37
3.2.4	Gruppe A: Verifizierter Schutz	37
3.2.4.1	Level A1: Verifizierter Entwurf.....	37
3.3	Grenzen und Schwächen der TCSEC	38
4	Die europäischen ITSEC und die deutschen ZSISC	41
4.1	Die Konzepte der ITSEC und ZSISC	42
4.1.1	Trennung von Funktionalität und Qualitätssicherung	43
4.1.2	Dreifaltige Evaluationsresultate.....	45
4.1.3	Ein Auswahlkatalog statt vorgeschriebener Funktionalität	46
4.2	Sicherheitsfunktionalität.....	46
4.2.1	Die verschiedenen Abstraktionsebenen in aktuellen Kriterien	47
4.2.2	Grundfunktionen	49
4.2.2.1	Die Grundfunktionen der ZSISC und ihre Defizite	49
4.2.2.2	Die Grundfunktionen der ITSEC und ihre Defizite	51
4.2.3	Funktionalitätsklassen.....	53
4.2.3.1	F-C2 als Beispiel einer ITSEC-Funktionalitätsklasse.....	54
4.2.3.2	COFC als Beispiel einer erweiterten ITSEC-Funktionalitätsklasse.....	57
4.2.4	Die Einseitigkeit der in den ZSISC und ITSEC berücksichtigten Funktionalität	59
4.3	Qualitätssicherung	59
4.3.1	Evaluation der Wirksamkeit.....	60
4.3.2	Evaluation der Korrektheit	61
4.3.3	Die ITSEC-Evaluationslevels	63
4.3.4	Probleme der Gestaltung der Evaluationslevels.....	64
4.3.5	Ein Beispiel nötiger und möglicher Änderungen im Bereich Qualitätssicherung	64
5	Bewertung der etablierten Zertifizierungs- und Kriterienszenarie	65
5.1	Eine Zusammenstellung der detaillierten Bewertungen.....	65
5.1.1	Balance der Sicherheitsfunktionalität	66
5.1.2	Balance der Qualitätssicherungsanforderungen.....	67
5.1.3	Kosten und Effizienz des Zertifizierungsprozesses.....	67
5.1.4	Aussagekraft und Verwertbarkeit der Ergebnisse	68
5.1.5	Entstehungsprozeß und Interpretation der Kriterien	68
5.2	Nutzen und Risiken von Zertifizierung und Kriterien	69
5.3	Verbesserungen durch neuere und andere Kriterien?	71

Teil C: Die Post-ITSEC-Kriterien	73
6 Die kanadischen CTCPEC.....	75
6.1 Sicherheitsfunktionalität.....	75
6.2 Qualitätssicherungsmaßnahmen	77
7 Die ISO/IEC-ECITS.....	79
7.1 Die Entwicklung seit 1990	79
7.2 Gliederung von Funktionalität in Weiterentwicklung der CTCPEC	81
8 Die Common Criteria	87
8.1 Die Federal Criteria und die Vorgeschichte der Common Criteria	87
8.2 Die Struktur der CC	88
8.2.1 Evaluationsergebnisse nach den CC	89
8.2.2 Schutzprofile in den CC	90
8.2.3 Sicherheitsfunktionalität in den CC	90
8.2.4 Qualitätssicherung in den CC.....	93
8.3 Die weitere Entwicklung der CC	95
9 Die Post-ITSEC-Kriterien im Lichte der ITSEC-Kritik	97
9.1 Balance der Sicherheitsfunktionalität	97
9.1.1 Berücksichtigung mehrseitiger Sicherheit	98
9.1.2 Verdeckte Kanäle.....	98
9.2 Balance der Qualitätssicherungsanforderungen.....	99
9.3 Kosten und Effizienz des Zertifizierungsprozesses	101
9.4 Aussagekraft und Verwertbarkeit der Ergebnisse	101
9.5 Entstehungsprozeß und Interpretation der Kriterien	102
9.6 Ein Zwischenfazit.....	104
Teil D: Konzepte für Kriterien für mehrseitig sichere Systeme	105
10 Eine neue Gliederung von Sicherheitsfunktionalität	107
10.1 Die bisherigen Gliederungen und ihre Defizite.....	107
10.2 Zweck und Struktur der neuen Gliederung	108
10.3 Ziele, Schutzprinzipien und funktionale Bausteine im einzelnen	110
10.3.1 Schutzprinzipien und funktionale Bausteine zum Ziel „Confidentiality“	110
10.3.2 Schutzprinzipien und funktionale Bausteine zum Ziel „Fitness for Use“	112
10.3.3 Schutzprinzipien und funktionale Bausteine zum Ziel „Accountability“	115
10.4 Die nicht mehr vertretenen CTCPEC- und ISO-ECITS-Services	117
11 Eine Funktionalitätsklasse für TK-Anlagen als Beispiel	121
11.1 Eine kurze Beschreibung der ITSEC-Funktionalitätsklasse.....	121
11.2 Diskussion und Ergänzungen der ITSEC-Funktionalitätsklasse	122
11.3 Abbildung der ITSEC-Funktionalitätsklasse in die neue Gliederung	124
11.4 Einordnung der gesamten Funktionalität in die neue Gliederung	129

11.4.1	Anforderungen zum Ziel „Confidentiality“	129
11.4.2	Anforderungen zum Ziel „Fitness for Use“	131
11.4.3	Anforderungen zum Ziel „Accountability“	133
Teil E: Organisation der Zertifizierung und der Weiterentwicklung ihrer fachlichen Grundlagen.....		135
12	Aufgaben der Organisation.....	137
12.1	Abgrenzung der Teilaufgaben	137
12.2	Annahmen zu Zielen und Rahmenbedingungen der Organisation	138
12.3	Zertifizierung	140
12.3.1	Antragsannahme, -vorprüfung und -verwaltung	140
12.3.2	Begleitung der Evaluation	142
12.3.3	Ausgabe des Zertifikates und des Zertifizierungsberichtes	143
12.3.4	Verwaltung von Zertifikaten	144
12.4	Evaluation	145
12.4.1	Prüfung des Evaluationsgegenstandes.....	145
12.4.2	Verfassung des Evaluationsberichtes	146
12.4.3	Beratung des Sponsors während der Evaluation	147
12.5	Akkreditierung der Evaluationsstellen.....	147
12.5.1	Annahme und Verwaltung von Akkreditierungsanträgen	147
12.5.2	Prüfung der potentiellen Evaluationsstellen	148
12.5.3	Fortlaufende Kontrolle der Qualität der Evaluationsstellen	150
12.6	Information und Beratung der Nicht-Insider	150
12.6.1	Informationen zu Zertifikaten und Zertifizierungsberichten	150
12.6.2	Informationen über die Zertifizierungssysteme.....	151
12.7	Weiterentwicklung von Kriterien und Methoden.....	152
12.7.1	Spezifische Ausarbeitung der Kriterien für spezielle Anwendungen.....	152
12.7.2	Verwaltung der spezifischen Ausarbeitungen	154
12.7.3	Überarbeitung der Kriterien.....	154
12.7.4	(Weiter-) Entwicklung und Harmonisierung von Evaluationsmethoden.....	155
13	Zertifizierung.....	157
13.1	Organisationsformen für Zertifizierungsstellen	157
13.1.1	Bestehende Organisationsformen und ihre Grenzen	157
13.1.2	Kombinationen der bestehenden Organisationsformen	158
13.1.3	Neue Organisationsmodelle.....	159
13.1.4	Einbettung in eine Rahmenorganisation.....	160
13.2	Die Organisationsformen im Lichte der Anforderungen	161
13.2.1	Antragsannahme, -vorprüfung und -verwaltung	162
13.2.2	Begleitung der Evaluation	164
13.2.3	Ausgabe des Zertifikates und des Zertifizierungsberichtes	165
13.2.4	Verwaltung von Zertifikaten	165

13.3 Kosten, Kostenverteilung und Haftung.....	166
13.3.1 Kosten und Kostenverteilung.....	166
13.3.2 Haftungsfragen	167
14 Evaluation	169
14.1 Organisationsformen für Evaluationsstellen	169
14.2 Die Organisationsformen im Lichte der Anforderungen	170
14.2.1 Prüfung des Evaluationsgegenstandes.....	170
14.2.2 Verfassung des Evaluationsberichtes	171
14.2.3 Beratung des Sponsors während der Evaluation	171
14.3 Kosten, Kostenverteilung und Haftung.....	172
14.3.1 Kosten und Kostenverteilung.....	172
14.3.2 Haftungsfragen	173
15 Akkreditierung der Evaluationsstellen	175
15.1 Organisationsformen für Akkreditierungsstellen.....	175
15.2 Die Organisationsformen im Lichte der Anforderungen	176
15.2.1 Annahme und Verwaltung von Akkreditierungsanträgen	176
15.2.2 Prüfung der potentiellen Evaluationsstellen	177
15.2.3 Fortlaufende Kontrolle der Qualität der Evaluationsstellen	178
15.3 Kosten, Kostenverteilung und Haftung.....	178
16 Information und Beratung der Nicht-Insider.....	181
16.1 Organisationsformen für Informations- und Beratungsstellen.....	181
16.1.1 Bestehende Organisationsformen	181
16.1.2 Neue Organisationsformen	182
16.2 Die Organisationsformen im Lichte der Anforderungen	182
16.2.1 Informationen zu Zertifikaten und Zertifizierungsberichten	183
16.2.2 Informationen über die Zertifizierungssysteme.....	183
16.3 Kosten, Kostenverteilung und Haftung.....	183
16.3.1 Kosten und Kostenverteilung.....	183
16.3.2 Haftungsfragen	184
17 Weiterentwicklung von Kriterien und Methoden.....	185
17.1 Spezifische Ausarbeitung der Kriterien für spezielle Anwendungen.....	185
17.1.1 Organisationsformen	185
17.1.2 Die Organisationsformen im Lichte der Anforderungen	186
17.1.3 Kosten und Kostenverteilung.....	186
17.2 Verwaltung der spezifischen Ausarbeitungen	186
17.2.1 Organisationsformen	186
17.2.2 Die Organisationsformen im Lichte der Anforderungen	187
17.2.3 Kosten und Kostenverteilung.....	188
17.3 Überarbeitung der Kriterien	188
17.3.1 Organisationsformen	188

17.3.2 Die Organisationsformen im Lichte der Anforderungen	189
17.3.3 Kosten und Kostenverteilung.....	190
17.4 Entwicklung und Harmonisierung von Evaluationsmethoden	190
17.4.1 Organisationsformen	190
17.4.2 Die Organisationsformen im Lichte der Anforderungen	191
17.4.3 Kosten und Kostenverteilung.....	191
Nachwort	193
Anhänge.....	195
Anhang A: Literatur.....	197
Anhang B: TK-Funktionalitätsklasse nach ITSEC.....	215
Anhang C: Stichwortverzeichnis	221
Anhang D: Abkürzungsverzeichnis	227

Abbildungsverzeichnis

Abb. 1-1:	Ablauf der Zertifizierung eines Produktes bzw. Systems und der Akkreditierung eines Prüflabors	7
Abb. 1-2:	In Deutschland an Evaluation, Zertifizierung und Akkreditierung beteiligte Instanzen	9
Abb. 1-3:	IT-Sicherheitsevaluationskriterien und ihre Editoren.....	17
Abb. 2-1:	Transitive Ausbreitung von Fehlern und Angriffen	23
Abb. 3-1:	Gruppen und Levels der TCSEC	35
Abb. 4-1:	Sicherheitsevaluation zweifach gegliedert in Bewertung der Funktionalität und der Qualitätssicherung.....	44
Abb. 4-2:	ITSEC- und TCSEC-Levels im Vergleich	45
Abb. 4-3:	Abstraktionsebenen von Sicherheitsfunktionalität.....	48
Abb. 4-4:	Die acht Sicherheitsgrundfunktionen der ZSISC (links) und die adressierten Problembereiche (rechts)	50
Abb. 4-5:	Die acht „Generic Headings“ der ITSEC (links) und die adressierten Problembereiche (rechts)	52
Abb. 4-6:	Phasen der Entwicklung und der Qualitätssicherung (gemäß ITSEC)	62
Abb. 5-1:	Nutzen und Risiken von Zertifizierung und Kriterien	69
Abb. 6-1:	Die vier „Facets / Functional Criteria“ und 18 „Security Services“ der CTCPEC	76
Abb. 6-2:	Die „Facets / Functional Criteria“ und „Security Services“ des CTCPEC-Ergänzungsentwurfs	77
Abb. 7-1:	Die 29 „Security Services“ der ECITS, geordnet nach den fünf „Categories“	82
Abb. 8-1:	„Classes“ und „Families“ zu „Functionality“ in Teil 2 der CC.....	92
Abb. 8-2:	„Classes“ und „Families“ zu „Assurance“ in Teil 3 der CC.....	94
Abb. 8-3:	Die 7 „Evaluation Assurance Levels“ (EAL) der CC.....	95
Abb. 10-1:	Gliederung sicherer Funktionalität in 3 Ziele, 8 Schutzprinzipien und 20 funktionale Bausteine	109