Nach intensiver internationaler Überarbeitung wird die Version 1.2 der ITSEC, mit Zustimmung der (informellen) EG-Beratergruppe SOG-IS (Senior Officials Group - Information Systems Security), zur Anwendung innerhalb des Evaluations- und Zertifizierungschemas für den vorläufigen Zeitraum von zwei Jahren ab Publikationsdatum, veröffentlicht. Die gewonnene praktische Erfahrung wird dazu verwendet, die ITSEC am Ende dieses Zeitraums zu überarbeiten und weiterzuentwickeln. Zusätzlich werden Hinweise, die sich aus der weiteren internationalen Harmonisierung ergeben, in Betracht gezogen.

INHALT

Seite

Abbildungen

0 EINLEITUNG

0.1 Die Informationstechnik (IT) hat im Verlauf von nur vier Jahrzehnten eine wichtige, oft sogar lebenswichtige Rolle in fast allen Bereichen jeder organisierten Gesellschaft eingenommen. Als Folge hieraus wurde Sicherheit ein entscheidender Bestandteil der Informationstechnik.

0.2 In diesem Zusammenhang bedeutet IT-Sicherheit

- **Vertraulichkeit** - Schutz vor unbefugter Preisgabe von Informationen;
- **Integrität** - Schutz vor unbefugter Veränderung von Informationen;
- **Verfügbarkeit** - Schutz vor unbefugter Vorenthaltung von Informationen oder Betriebsmitteln.

0.3 An jedes **IT-System** oder **-Produkt** werden eigene Anforderungen bezüglich der Einhaltung von Vertraulichkeit, Integrität und Verfügbarkeit gestellt. Um diese Anforderungen zu erfüllen, enthält es eine Reihe technischer Sicherheitsmaßnahmen, in diesem Dokument als **sicherheitsspezifische** Funktionen bezeichnet, beispielsweise für die Zugriffskontrolle, die Protokollauswertung und die Fehlerüberbrückung. Gefordert wird ein angemessenes Vertrauen in diese Funktionen: Das wird im vorliegenden Dokument als **Vertrauenswürdigkeit** bezeichnet, unabhängig davon, ob es sich um das Vertrauen in die **Korrektheit** der sicherheitsspezifischen Funktionen (sowohl vom Gesichtspunkt der Entwicklung als auch von dem des Betriebs) oder um das Vertrauen in die **Wirksamkeit** dieser Funktionen handelt.

0.4 Die Benutzer von Systemen müssen sich auf die Sicherheit des von ihnen verwendeten Systems verlassen können. Sie benötigen auch einen Maßstab für den Vergleich der Sicherheitseigenschaften von IT-Produkten, deren Anschaffung sie in Betracht ziehen. Ein Benutzer könnte sich auf das Wort des Herstellers oder Vertreibers der betreffenden Systeme oder Produkte verlassen oder sie selbst testen, aber viele Benutzer vertrauen eher dem Ergebnis einer neutralen Bewertung durch eine unabhängige Stelle. Eine solche **Evaluation** von Systemen oder Produkten erfordert objektive und genau definierte Kriterien für die Bewertung der Sicherheit und das Vorhandensein einer **Zertifizierungsstelle**, die bestätigen kann, daß die Evaluation ordnungsgemäß durchgeführt wurde. Die **Sicherheitsvorgaben** für Systeme sind speziell auf die besonderen Notwendigkeiten des Nutzers ausgerichtet, während die Sicherheitsvorgaben für Produkte allgemeiner sein werden, so daß Produkte, die sie erfüllen, in vielen Systemen mit ähnlichen, aber nicht identischen Sicherheitsanforderungen eingesetzt werden können.

0.5 Für ein System kann die Bewertung seiner Sicherheitseigenschaften als Teil einer Abnahmeprozedur gesehen werden, die den Betrieb des Systems in seiner speziellen Umgebung genehmigt. **Akkreditierung** ist der häufig für diese Prozedur verwendete Begriff. Verschiedene Faktoren müssen berücksichtigt werden, um zu beurteilen, ob ein System für seinen Einsatzzweck geeignet ist. Dazu gehören: Vertrauen in die Sicherheit, die das System bietet, eine Bestätigung der Verantwortung des Managements für die Sicherheit, Übereinstimmung mit relevanten technischen und juristischen Anforderungen

sowie Vertrauen in die Angemessenheit anderer, nicht technischer Sicherheitsmaßnahmen, die in der Systemumgebung getroffen worden sind. Die Kriterien, die in diesem Dokument beschrieben sind, betreffen in erster Linie technische Sicherheitsmaßnahmen, aber sie sprechen auch einige nichttechnische Aspekte an, wie z.B. Vorschriften für die personelle, materielle und organisatorische Sicherheit (aber nur dann, wenn sich daraus ein Einfluß auf die technischen Sicherheitsmaßnahmen ergibt).

0.6 Bei der Entwicklung von Kriterien für die Bewertung der Sicherheit von IT-Systemen wurde zwar schon viel geleistet, doch hatten diese Kriterien je nach den Anforderungen der beteiligten Länder oder Stellen voneinander abweichende Zielsetzungen. Die wichtigsten Kriterien dabei - und daneben auch in vielen Punkten ein Vorläufer für andere Entwicklungen - waren die "Trusted Computer System Evaluation Criteria" [TCSEC], bekannt als "Orange Book", die durch das US-Verteidigungsministerium herausgegeben und für die Produktevaluation genutzt werden. Andere, meist europäische Länder verfügen ebenfalls über beträchtliche Erfahrungen in der IT-Sicherheitsevaluation und haben eigene IT-Sicherheitskriterien entwickelt. In Großbritannien fallen hierunter u.a. das "CESG Memorandum Nr. 3" [CESG3], das für die Verwendung durch Regierungsstellen entwickelt wurde, sowie Vorschläge aus dem Handels und Industrieministerium, das "Grüne Buch" [DTIEC], für kommerzielle IT-Sicherheitsprodukte. In Deutschland hat die Zentralstelle für Sicherheit in der Informationstechnik - jetzt Bundesamt für Sicherheit in der Informationstechnik - im Jahre 1989 eine erste Fassung ihrer eigenen Kriterien veröffentlicht [ZSIEC], während in Frankreich gleichzeitig Kriterien, das sogenannte "Blau-weiß-rote Buch" [SCSSI], entwickelt wurden.

0.7 Angesichts der Entwicklung in diesem Bereich und der weiterreichenden Bedürfnisse erkannten Frankreich, die Bundesrepublik Deutschland, die Niederlande und Großbritannien, daß diese Arbeiten in einer abgestimmten Art und Weise durchgeführt und gemeinsame, harmonisierte IT-Sicherheitskriterien angestrebt werden sollten. Für diese Harmonisierung gab es drei Gründe:

a) in den unterschiedlichen Ländern waren schon viele Erfahrungen gesammelt worden und eine gemeinsame Nutzung dieser Erfahrungen wäre für alle Beteiligten gewinnbringend;

b) die Industrie lehnte es ab, verschiedene Sicherheitskriterien in den verschiedenen Ländern vorzufinden;

c) die grundlegenden Konzepte und Ansätze waren über alle Länder und selbst bei kommerziellen, amtlichen und verteidigungstechnischen Anwendungen gleich.

0.8 Aus diesem Grunde wurde beschlossen, auf den verschiedenen nationalen Initiativen aufzubauen, die besten Teile der bereits geleisteten Arbeiten aufzugreifen und sie in eine in sich geschlossene, strukturierte Darstellung einzubringen. Besonderer Wert wurde dabei darauf gelegt, daß möglichst breite Anwendbarkeit und Übereinstimmung mit bereits vorliegenden Arbeiten, insbesondere mit den amerikanischen TCSEC erreicht wird. Ursprünglich wollte man sich auf die Harmonisierung bereits vorliegender Kriterien beschränken, doch war es manchmal erforderlich, das vorhandene Material zu ergänzen.

0.9 Ein Grund für die Erarbeitung dieser international harmonisierten Kriterien besteht darin, innerhalb der vier zusammenarbeitenden Länder eine einheitliche Grundlage für die **Zertifizierung** durch die nationalen Zertifizierungsstellen zur Verfügung zu stellen, mit dem Ziel der gegenseitigen Anerkennung von Evaluationsergebnissen.

0.10 Dieses Dokument enthält die harmonisierten Kriterien. Kapitel 1 enthält eine kurze Darstellung des Umfangs der harmonisierten Kriterien. Kapitel 2 behandelt die Sicherheitsfunktionalität, d.h. die Definition und Beschreibung der Sicherheitsanforderungen. Kapitel 3 definiert Kriterien, nach denen das Vertrauen in die Wirksamkeit eines **Evaluationsgegenstandes** bewertet werden soll, der die formulierten Sicherheitsanforderungen implementiert. In Kapitel 4 wird dieser Aspekt auf die Betrachtung der Korrektheit der Lösung ausgedehnt. Kapitel 5 beschreibt die zulässigen Ergebnisse einer Evaluation und Kapitel 6 enthält das Glossar der Begriffe, die innerhalb dieser Kriterien eine genauer festgelegte oder möglicherweise vom normalen deutschen Sprachgebrauch abweichende Bedeutung haben. (Beim ersten Auftreten werden diese Begriffe fett gedruckt; Kursive Schrift wird zur Hervorhebung eingesetzt). Dieses Glossar soll dem Leser nicht nur dabei helfen, ihm das Verständnis dieser Begriffe zu erleichtern, sondern, es soll ihm auch Ideen und Konzepte vermitteln, die den harmonisierten Kriterien zu eigen sind.

0.11 Die Evaluationskriterien in den Kapiteln 3 und 4 sind in einer einheitlichen Form aufgebaut. Darin wird festlegt, was vom **Antragsteller** der Evaluation (die Person oder Organisation, die eine Evaluation beantragt) zur Verfügung gestellt werden muß und was vom **Evaluator** (die unabhängige Person oder Organisation, die die Evaluation durchführt) getan werden muß. Diese Einteilung soll zur Konsistenz und Einheitlichkeit von Evaluationsergebnissen beitragen. Zu jedem Abschnitt der Evaluation wird die Dokumentation aufgeführt, die vom Antragsteller zur Verfügung gestellt werden muß. Darauf folgen dann die Kriterien für jeden Aspekt oder für jede Phase, die für die Evaluation dieses Abschnitts zutreffen. Die Kriterien bestehen aus **Anforderungen an Inhalt und Form** der Dokumentation, die vom Antragsteller zur Verfügung gestellt werden muß, aus den **Anforderungen zum Nachweis** des geforderten Inhalts der Dokumente und aus den **Aufgaben des Evaluators**, die von diesem durchgeführt werden müssen, um sowohl die zur Verfügung gestellten Dokumente zu prüfen als auch, wo erforderlich, zusätzliche Tests oder andere Tätigkeiten durchzuführen. Im Fall von Kriterien, die die Anwendung des Systems oder des Produkts im Betrieb betreffen, wird der Antragsteller im allgemeinen nicht in der Lage sein, einen Nachweis über die wirkliche Nutzung zur Verfügung zu stellen. Aus diesem Grund muß der Evaluator für die laufende Evaluation annehmen, daß die Verfahren, die vom Antragsteller beschrieben werden, in der Praxis auch durchgeführt werden.

0.12 In den Kriterien werden einige Verben in einer besonderen Weise benutzt. *"muß/müssen"* wird benutzt, um auszudrücken, daß die Kriterien erfüllt werden müssen; *"kann/können"* wird benutzt, um auszudrücken, daß die Kriterien nicht unbedingt einzuhalten sind und *"wird/werden"* wird benutzt, um Tätigkeiten auszudrücken, die in Zukunft stattfinden. In ähnlicher Weise werden die Verben *"angeben"*, *"beschreiben"* und *"erklären"* in den Kriterien benutzt, um den Nachweis eines Sachverhaltes mit

zunehmender Strenge zu fordern. *Angeben* bedeutet, daß die relevanten Fakten zur Verfügung gestellt werden müssen; *beschreiben* bedeutet, daß die Fakten zur Verfügung gestellt werden müssen und daß ihre relevanten Eigenschaften aufgezählt werden müssen; *erklären* bedeutet, daß die Fakten zur Verfügung gestellt, ihre relevanten Eigenschaften aufgezählt und Begründungen gegeben werden müssen.

0.13 Bis auf Kapitel 4 sind die Paragraphen in jedem Kapitel fortlaufend durchnumeriert. In Kapitel 4 sind die Kriterien für jede Evaluationsstufe getrennt dargestellt. Die einführenden Paragraphen dieses Kapitels sind wie in den anderen Kapiteln numeriert, aber dann sind die Paragraphen der Kriterien für jede Evaluationsstufe fortlaufend durchnumeriert, wobei unter der gleichen Paragraphennummer in jeder Evaluationsstufe das gleiche Thema behandelt wird. Jeder Paragraph in dem Dokument kann trotzdem durch die Angabe von Kapitelnummer oder Stufennummer und der Nummer des Paragraphen eindeutig identifiziert werden.

0.14 Diese Arbeit baut auf Dokumenten auf, die in der Praxis bereits umfassend diskutiert und verwendet wurden; darüber hinaus kann gesagt werden, daß die Ideen und Konzepte sorgfältig gegeneinander abgewogen wurden und der für die Kriterien gewählte Aufbau eine bestmögliche Konsistenz gewährleistet und eine möglichst einfache Handhabung erlaubt. Die vorliegende Fassung der ITSEC hat viel von der Kritik profitiert, die in dem internationalen Abstimmungsprozeß geäußert worden ist. Der Abstimmungsprozeß ist durch die Kommission der Europäischen Gemeinschaft unterstützt worden, die eine Konferenz organisierte, auf der die Version 1.0 diskutiert wurde, und eine darauffolgende Arbeitstagung, bei der die Zwischenversion (Version 1.1) weiter verfeinert wurde. Diese Aktivitäten wurden durch schriftliche Kommentare ergänzt, die von den Autoren beim Entwurf der Version 1.2 so weit wie möglich berücksichtigt wurden.

0.15 Es wird daher erwartet, daß diese Kriterien auf breiter Front akzeptiert und bei vielen potentiellen Benutzern und in vielen Wirtschaftsbereichen Verwendung finden werden; man ist sich allerdings darüber im klaren, daß es Verbesserungen geben kann und wird. Kommentare und Vorschläge sind erwünscht und unter Angabe des Vermerks "ITSEC-KOMMENTARE" an eine der folgenden Anschriften zu richten:

Commission of the European Communities
Directorate XIII/F
SOG-IS Secretariat
Rue de la Loi 200
B-1049 BRUSSELS

In Frankreich:

Service Central de la Sécurité des Systèmes d'Information
Division Information et Systèmes
18 rue du Docteur Zamenhof
F-92131 ISSY LES MOULINEAUX

In Deutschland:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
D-5300 BONN 2

In den Niederlanden:

Netherlands National Comsec Agency
Bezuidenhoutseweg 67
P.O. Box 20061
NL-2500 EB THE HAGUE

In Großbritannien:

Head of the Certification Body
UK IT Security Evaluation and Certification Scheme
Room 2/0805
Fiddlers Green Lane
CHELTENHAM
Glos GB-GL52 5AJ

0.16 Kopien der durch die EG veröffentlichten ITSEC Version 1.2 sind bei der EG-Kommission unter der obigen Adresse erhältlich.

1 Anwendungsbereich

Technische Sicherheitsmaßnahmen

1.1 Ein Großteil der Sicherheit eines IT-Systems kann oft durch nicht-technische Maßnahmen wie beispielsweise organisatorische, personelle, materielle oder administrative Maßnahmen realisiert werden. Die Tendenz und die Notwendigkeit zum Einsatz technischer IT-Sicherheitsmaßnahmen nimmt aber zu. Obgleich die nachfolgenden Kriterien vor allem technische Sicherheitsmaßnahmen betreffen, sprechen sie einige nicht-technischen Aspekte an, insbesondere die zugehörigen Vorschriften für die personelle, materielle und organisatorische Sicherheit, die für den Betrieb der Systeme oder Produkte gelten (aber nur insoweit, als sie beim Betrieb Einfluß auf die technischen Sicherheitsmaßnahmen haben).

1.2 Diese Kriterien wurden so angelegt, daß sie in wesentlichen Teilen für technische Sicherheitsmaßnahmen anwendbar sind, unabhängig davon, ob sie in Hardware, Software oder Firmware realisiert sind. Wo besondere Aspekte der Evaluation nur auf bestimmte Arten der Realisierung angewendet werden sollen, wird dies als Teil der betreffenden Kriterien beschrieben.

1.3 Diese Kriterien behandeln keine physikalischen Aspekte der Sicherheit von Hardware, wie z.B. einbruchssichere Gehäuse oder die Überwachung elektromagnetischer Abstrahlung.

Systeme und Produkte

1.4 Für die Zwecke des vorliegenden Dokuments kann der Unterschied zwischen Systemen und Produkten wie folgt erläutert werden: Ein *IT-System* ist eine spezielle IT-Installation mit einem definierten Zweck und einer bekannten Einsatzumgebung. Bei einem *IT-Produkt* handelt es sich um ein Hardware- und/oder Softwarepaket, das "von der Stange" gekauft und in eine Vielzahl von Systemen eingebaut werden kann. Ein IT-System setzt sich im allgemeinen aus mehreren Hardware- und Software-**Komponenten** zusammen. Einige dieser Komponenten (z.B. Anwendungssoftware) sind gewöhnlich speziell entwickelt worden, während andere Komponenten (z.B. Hardware) üblicherweise Standardprodukte sein werden. Für bestimmte Anwendungsfälle wird es möglich sein, ein einzelnes Produkt zu kaufen, das dann als vollständiges System eingesetzt werden kann, aber normalerweise wird zumindest ein gewisses Maß von Anpassung und Integration notwendig sein, um die systemspezifischen Forderungen zu erfüllen.

1.5 Vom Standpunkt der Sicherheit liegt also der Hauptunterschied zwischen Systemen und Produkten in der unterschiedlichen Kenntnis bezüglich ihrer Einsatzumgebung. Ein System wurde entwickelt, um die Forderungen einer bestimmten Gruppe von **Endnutzern** zu erfüllen. Es besitzt eine reale Einsatzumgebung, die genau definiert und beobachtet werden kann; insbesondere sind die Eigenschaften und Anforderungen

seiner Endnutzer bekannt und die Bedrohungen seiner Sicherheit sind reale Bedrohungen, die bestimmt werden können. Ein Produkt hingegen muß für den Einbau in viele Systeme geeignet sein, bei seiner Entwicklung können nur allgemeine Annahmen über die Einsatzumgebung des Systems gemacht werden, dessen Teil es möglicherweise werden soll. Wer das Produkt kauft und das System zusammensetzt, muß sicherstellen, daß diese Annahmen mit der wirklichen Umgebung des Systems übereinstimmen.

1.6 Aus Gründen der Konsistenz ist es wichtig, sowohl für Produkte als auch für Systeme dieselben Sicherheitskriterien anzuwenden; es ist dann einfacher und kostengünstiger, Systeme zu bewerten, die bereits erfolgreich evaluierte Produkte enthalten. Aus diesem Grund befassen sich die vorstehenden Kriterien mit der Bewertung der Sicherheit sowohl von IT-Produkten als auch von IT-Systemen. Im weiteren Verlauf dieses Dokuments wird der Begriff "Evaluationsgegenstand" (EVG) für ein zu bewertendes Produkt oder System verwendet.

1.7 Ein EVG kann aus mehreren Komponenten bestehen. Einige dieser Komponenten werden für die **Sicherheitsziele** des EVG ohne Bedeutung sein. Andere jedoch werden unmittelbar dazu beitragen, daß die Sicherheitsziele erreicht werden. Diese Komponenten werden als sicherheitsspezifisch bezeichnet. Schließlich kann es einige Komponenten geben, die nicht sicherheitsspezifisch sind, die aber korrekt arbeiten müssen, damit die Sicherheit des EVG gewährleisten kann; sie werden als **sicherheitsrelevant** bezeichnet. Sicherheitsspezifische und sicherheitsrelevante Komponenten, die zusammen für die Sicherheit des EVG von Bedeutung sind, werden häufig als "Trusted Computing Base" (TCB) bezeichnet (siehe Abbildungen 1 und 2).

1.8 Der Hauptanteil an der Evaluation wird sich auf die Komponenten des EVG konzentrieren, die als sicherheitsspezifisch oder sicherheitsrelevant ausgewiesen sind; aber auch alle anderen Komponenten innerhalb des EVG müssen im Rahmen der Evaluation untersucht werden, um nachzuweisen, daß sie weder sicherheitsspezifisch noch sicherheitsrelevant sind.

Funktionalität und Vertrauenswürdigkeit, Klassen und Stufen

1.9 Damit ein EVG seine Sicherheitsziele erreichen kann, muß er geeignete sicherheitsspezifische Funktionen enthalten, beispielsweise für Bereiche wie Zugriffskontrolle, Protokollauswertung und Fehlerüberbrückung.

1.10 Diese Funktionen sind in einer Art und Weise zu definieren, die sowohl dem Antragsteller einer Evaluation als auch dem unabhängigen Evaluator klar und verständlich ist. Sie können entweder individuell spezifiziert oder durch Verweis auf eine vordefinierte **Funktionalitätsklasse** definiert werden. Die vorliegenden Kriterien enthalten zehn Beispiele solcher Funktionalitätsklassen. Diese Beispiele bauen auf den Klassen auf, die in den deutschen Kriterien [ZSIEC] definiert sind. Darin enthalten sind fünf Klassen, die sich eng an die Funktionalitätsanforderungen der amerikanischen Trusted Computer System Evaluation Criteria [TCSEC] anlehnen.

1.11 In jedem Fall muß der Antragsteller einer Evaluation die Sicherheitsvorgaben für die Evaluation definieren. Darin sind die sicherheitsspezifischen Funktionen des EVG zu definieren sowie weitere relevante Angaben festzuhalten, wie z.B. die Sicherheitsziele des EVG und die erwarteten **Bedrohungen**. Einzelheiten über bestimmte **Sicherheitsmechanismen**, die zur Realisierung der sicherheitspezifischen Funktionen eingesetzt werden, können angegeben werden.

1.12 Die zur Erreichung der Sicherheitsziele eines EVG gewählten sicherheitsspezifischen Funktionen stellen nur einen Aspekt der Sicherheitsvorgaben eines Produktes oder Systems dar. Nicht weniger bedeutend ist das Vertrauen, daß die ausgewählten sicherheitsspezifischen Funktionen und Mechanismen die Sicherheitsziele auch tatsächlich erreichen.

1.13 Der Gesichtspunkt des Vertrauens muß von mehreren Seiten betrachtet werden. Für diese harmonisierten Kriterien wurde entschieden, das Vertrauen in die Korrektheit der Implementierung von sicherheitsspezifischen Funktionen und Mechanismen von dem Vertrauen in ihre Wirksamkeit zu unterscheiden.

1.14 Bei der Evaluation der Wirksamkeit wird beurteilt, ob die sicherheitsspezifischen Funktionen und Mechanismen, die durch den EVG zur Verfügung gestellt werden, wirklich die vorgegebenen Sicherheitsziele erreichen. Der EVG wird hinsichtlich der **Eignung der Funktionalität**, des **Zusammenwirkens der Funktionen** (ob die ausgewählten Funktionen synergetisch zusammenarbeiten), der Konsequenzen von bekannten und entdeckten **Schwachstellen** (sowohl bei der Entwicklung des EVG als auch bei der Art und Weise, wie er im echten Betrieb genutzt wird) und der **Einfachheit der Anwendung** beurteilt.

1.15 Zusätzlich wird bei der Bewertung der Wirksamkeit die Fähigkeit der Sicherheitsmechanismen des EVG, Widerstand gegen einen direkten Angriff zu leisten, bewertet (**Stärke des Mechanismus**). Für die Stärke der Mechanismen sind drei Stufen definiert - niedrig, mittel, hoch -, die ein Maß für das Vertrauen sind, inwieweit die Sicherheitsmechanismen des EVG in der Lage sind, direkten Angriffen zu widerstehen.

1.16 Bei der Bewertung der Korrektheit wird untersucht, ob die sicherheitsspezifischen Funktionen und Mechanismen korrekt implementiert sind. Sieben Evaluationsstufen (E0 bis E6) wurden definiert, die verschiedene Stufen des Vertrauens in die Korrektheit darstellen. E0 bedeutet unzureichendes Vertrauen. E1 steht für einen Einstiegspunkt, unterhalb dessen kein sinnvolles Vertrauen aufrechtzuerhalten ist und E6 steht für die höchste Stufe des Vertrauens. Die anderen Stufen stellen Zwischenstufen dar. Die Korrektheit wird aus der Sicht der **Konstruktion** des EVG - darunter fallen sowohl der **Entwicklungsvorgang** als auch die **Entwicklungsumgebung** - sowie aus der Sicht des **Betriebs** des EVG betrachtet.

1.17 Die Evaluationsstufen werden im Zusammenhang mit den Korrektheitskriterien definiert. Die Anforderungen an die Wirksamkeit (einschließlich der Stärke der Mechanismen) ändern sich zwischen den Stufen nicht. Bei der Bewertung der Wirksamkeit wird auf der Bewertung der Korrektheit aufgebaut und es werden die vom Antragsteller zur

Verfügung gestellten Dokumente verwendet; in der Praxis werden sich die Bewertung der Korrektheit und der Wirksamkeit natürlich überlappen.

1.18 Wenn ein EVG irgendeinen Aspekt einer Evaluationsstufe wegen fehlender Information oder aus einem anderen Grunde nicht erfüllt, muß der Mangel entweder behoben werden oder der EVG muß von der Evaluation für diese Stufe zurückgezogen werden. Sonst erhält der EVG das Evaluationsergebnis E0.

1.19 Mit den sechs erfolgreichen Evaluationsstufen E1 bis E6 wird ein weiter Bereich von möglichem Vertrauen erfaßt. Nicht alle diese Stufen werden notwendigerweise für alle Bereiche des Marktes, die eine unabhängige Evaluation der technischen Sicherheitsmaßnahmen erfordern, benötigt oder sind für sie geeignet. Nicht alle Kombinationen von Funktionalität und Vertrauen werden notwendigerweise vernünftig oder nützlich sein. In der Regel wird zum Beispiel ein geringes Vertrauen in die Funktionalität nicht zur Erfüllung der militärischen Forderungen nach der gleichzeitigen Verarbeitung von Informationen unterschiedlicher Geheimhaltungsgrade passen. Es ist auch unwahrscheinlich, daß hohes Vertrauen in die Korrektheit eines EVG mit einer Anforderung nach geringer Mechanismenstärke kombiniert wird.

1.20 Diese harmonisierten Kriterien sind keine Richtlinie für den Entwurf sicherer Produkte oder Systeme. Es ist Sache des Antragstellers einer Evaluation, die Sicherheitsziele für seinen EVG festzulegen und die sicherheitsspezifischen Funktionen auszuwählen, mit denen die Sicherheitsziele erreicht werden. Jedoch können für jede Evaluationsstufe die Kriterien für das Vertrauen in die Korrektheit und Wirksamkeit als eine zu erfüllende Sicherheits-Checkliste angesehen werden.

Vertrauensprofile

1.21 Die Kriterien in diesem Dokument verlangen vom Antragsteller, daß er die gewünschte Evaluationsstufe als Teil der Sicherheitsvorgaben angibt. Alle in den Sicherheitsvorgaben aufgeführten sicherheitsspezifischen Funktionen werden dann daraufhin untersucht, ob sie gleichermaßen das Vertrauen rechtfertigen, welches durch diese Evaluationsstufe gefordert wird.

1.22 Für einige EVG kann die Forderung bestehen, daß einige sicherheitsspezifischen Funktionen ein höheres Vertrauen als andere bieten; z.B. können einige sicherheitsspezifischen Funktionen für den speziellen Anwendungsfall wichtiger sein als andere. Unter diesen Umständen ist es dem Antragsteller anheim gestellt, mehrere unterschiedliche Exemplare von Sicherheitsvorgaben für den EVG vorzulegen. Es würde den Rahmen dieser Kriterien sprengen, wenn man ausführen sollte, wie und unter welchen Bedingungen dies möglich ist.

Das Evaluationsverfahren

1.23 Ziel des Evaluationsverfahrens ist es, daß der Evaluator einen unparteiischen Bericht darüber abgeben kann, ob ein EVG seine Sicherheitsvorgaben mit dem Grad des Vertrauens erfüllt, der durch die beantragte Evaluationsstufe vorgegeben ist.

1.24 Das Evaluationsverfahren wird in Abbildung 3 dargestellt. Es erfordert die enge Einbeziehung des Antragstellers der Evaluation. Je höher die Evaluationsstufe, desto intensiver muß der Antragsteller mit einbezogen werden. Sowohl Nutzer als auch Hersteller können Antragsteller für Evaluationen sein. Eine Systemevaluation wird wahrscheinlich von dem zukünftigen Endnutzer des Systems oder seinem technischen Beauftragten in Auftrag gegeben und die Evaluation eines Produktes wird wahrscheinlich vom Hersteller des Produktes oder seinem Vertreiber in Auftrag gegeben, aber das muß nicht so sein. Jeder, der die erforderlichen technischen Informationen zur Verfügung stellen kann, kann eine Evaluation in Auftrag geben.

1.25 Zunächst muß der Antragsteller die Anforderungen für den Betrieb festlegen und die Bedrohungen identifizieren, denen der EVG widerstehen soll. Im Falle eines Systems ist es notwendig, die reale Betriebsumgebung für das System zu untersuchen, um die relevanten Bedrohungen zu ermitteln, denen zu begegnen ist. Bei einem Produkt ist zu entscheiden, welchen Bedrohungen das Produkt begegnen soll. Es wird davon ausgegangen, daß Industrieverbände und internationale Standardisierungsgremien im Laufe der Zeit Standardfunktionalitätsklassen als Grundlage für die Sicherheitsvorgaben für Produkte festlegen werden. Produktentwickler, die keine vordefinierte Marktnische oder besondere Arten von Anwendern im Blick haben, werden dabei möglicherweise feststellen, daß solche vordefinierten Funktionalitätsklassen eine gute Basis für Sicherheitsvorgaben darstellen, nach denen sie ihre Produkte entwickeln können.

1.26 Die Sicherheitsziele für den EVG können dann unter Berücksichtigung der rechtlichen und sonstigen Bestimmungen festgelegt werden. Sie legen den Beitrag zur Sicherheit fest (Vertraulichkeit, Integrität und Verfügbarkeit), den der EVG leisten soll. Ausgehend von den Sicherheitszielen können dann - möglicherweise schrittweise - die sicherheitsspezifischen Funktionen zusammen mit der angestrebten Evaluationsstufe für den EVG festgelegt werden, die der EVG erreichen muß, um das erforderliche Vertrauen zu rechtfertigen.

1.27 Die Ergebnisse dieser Arbeit - die Definition der sicherheitsspezifischen Funktionen, die erkannten Bedrohungen, die angegebenen Sicherheitsziele und speziell anzu-wendende Sicherheitsmechanismen - bilden die Sicherheitsvorgaben für die Entwicklung.

1.28 Für jede Evaluationsstufe werden durch die Kriterien die Unterlagen genannt, die der Antragsteller dem Evaluator zur Verfügung stellen muß. Der Antragsteller muß sicherstellen, daß diese Unterlagen bereitgestellt werden. Außerdem muß er darauf achten, daß alle Anforderungen bezüglich Inhalt und Form erfüllt sind und daß die Unterlagen den geforderten Nachweis wirklich erbringen oder die Erstellung eines solchen Nachweises unterstützen.

1.29 Damit eine Evaluation wirkungsvoll und mit minimalen Kosten durchgeführt werden kann, muß der Evaluator eng mit dem Entwickler und dem Antragsteller für den EVG zusammenarbeiten. Ideal ist eine Zusammenarbeit von Anbeginn der Entwicklung an, um ein gutes Verständnis für die Sicherheitsvorgaben zu entwickeln und um auf die Auswirkungen bestimmter Entscheidungen für die Evaluation hinweisen zu können. Der Evaluator muß aber unabhängig bleiben und darf nicht vorschlagen, wie ein EVG entworfen oder implementiert werden soll. Dies ist vergleichbar mit der Rolle eines externen Finanzrevisors, der eine gute Arbeitsbeziehung mit der Finanzabteilung aufbauen muß und der in vielen Fällen von deren internen Aufzeichnungen und Kontrollen nach ihrer Prüfung Gebrauch macht. Trotzdem muß auch er unabhängig und kritisch bleiben.

1.30 Die Forderungen nach Sicherheitstests und Analysen in den Kriterien verdienen besondere Erwähnung; in allen Fällen liegt die Verantwortung für Test und Analyse beim Antragsteller. Für alle Evaluationsstufen, mit Ausnahme von E1, wird der Evaluator vorrangig die Test- und Analyseergebnisse überprüfen, die der Antragsteller zur Verfügung gestellt hat. Der Evaluator wird eigene Test- und Analysearbeiten nur durchführen, um die gelieferten Ergebnisse zu überprüfen, die gelieferten Nachweise zu ergänzen und um Schwachstellen zu untersuchen. Bei der Evaluierungsstufe E1 ist es freigestellt, ob Testergebnisse zur Verfügung gestellt werden oder nicht. Ist dies nicht der Fall, so muß der Evaluator zusätzlich Funktionalitätstests gegen die Sicherheitsvorgaben durchführen.

Der Zertifizierungsprozeß

1.31 Damit die Kriterien einen praktischen Wert haben, müssen sie durch Vorschriften für die Durchführung und Überwachung von unabhängigen Evaluationen, die durch qualifizierte und anerkannte nationale Zertifizierungsstellen durchgeführt werden, ergänzt werden. Diese Stellen werden Zertifikate vergeben, in denen die **Bewertung** der Sicherheit des EVG bestätigt wird, welche er auf Grund einer ordnungsgemäß durchgeführten Evaluation erreicht hat. Sie werden Prozeduren genehmigen, wie von den Kriterien gefordert, die die Authentizität des ausgelieferten EVG garantieren. Sie werden ebenfalls für die Auswahl und für die Überwachung von zugelassenen Evaluatoren verantwortlich sein. Die Beschreibung der Verfahren, nach denen solche Stellen arbeiten, liegt außerhalb des Rahmens dieser Kriterien.

1.32 Diese Kriterien wurden so angelegt, daß die Subjektivität, die sich bei Evaluationen nicht vermeiden läßt, möglichst gering gehalten werden kann. Es wird in der Verantwortung der nationalen Zertifizierungsstellen liegen, die Einheitlichkeit der zertifizierten Evaluationsergebnisse sicherzustellen. Wie das erreicht wird, liegt außerhalb des Rahmens dieser Kriterien.

1.33 Damit die Ergebnisse einer Evaluation, die nach diesen Kriterien durchgeführt wurde, von einer nationalen Zertifizierungsstelle zertifiziert werden können, muß der Evaluator einen Bericht erstellen, der die Ergebnisse der Evaluation in einer Form enthält, die eine Zertifizierung ermöglicht. Die Beschreibung des genauen Aufbaus und des Inhalts von Evaluationsberichten liegt außerhalb des Rahmens dieser Kriterien.

1.34 Die meisten Sicherheitsvorgaben und EVG werden sich im Laufe der Zeit ändern. Wie ein Zertifikat nach Änderungen am EVG (ob sicherheitsrelevant oder nicht) oder bei Änderungen der Sicherheitsvorgaben (wie z.B. neue Bedrohungen oder Sicherheitsziele) behandelt wird, wird durch die jeweiligen nationalen Zertifizierungsstellen geregelt. Eine erneute Evaluation (Reevaluation) wird unter bestimmten Umständen erforderlich werden, unter anderen nicht. Die Beschreibung der entsprechenden Regeln und Verfahren liegt ebenfalls außerhalb des Rahmens dieser Kriterien.

Verhältnis zu den TCSEC

1.35 Die "Trusted Computer System Evaluation Criteria" [TCSEC], allgemein als TCSEC oder "Orange Book" bekannt, stellen die weithin bekannte und anerkannte Grundlage für die Bewertung der Sicherheit von Betriebssystemen dar. Nachdem sie erstmals im Jahre 1983 veröffentlicht worden sind, werden sie vom amerikanischen Verteidigungsministerium im Rahmen des amerikanischen Verfahrens zur Produktevaluation durch das "National Computer Security Center" (NCSC), angewendet. Die TCSEC sind so angelegt, daß sie der IT-Sicherheitspolitik des amerikanischen Verteidigungsministeriums entsprechen. Diese Politik hat im wesentlichen das Ziel, die Vertraulichkeit von Informationen zu gewährleisten, die dem staatlichen Geheimschutz unterliegen.

1.36 Die TCSEC definieren sieben verschiedene Mengen Evaluationskriterien, die Klassen genannt werden (D, C1, C2, B1, B2, B3 und A1) und die in vier Gruppen zusammengefaßt sind (D, C, B und A). Jede Kriterienklasse umfaßt vier Aspekte der Evaluation: Sicherheitspolitik, Beweissicherung, Vertrauenswürdigkeit und Dokumentation. Die Kriterien für diese vier Aspekte werden von Klasse zu Klasse detaillierter und bilden eine Hierarchie, in welcher D die niedrigste und A1 die höchste Klasse darstellt. Jede dieser Klassen beinhaltet sowohl Forderungen an die Funktionalität als auch an die Vertrauenswürdigkeit.

1.37 Die im vorliegenden Dokument enthaltenen Kriterien ermöglichen die Auswahl beliebiger sicherheitsspezifischer Funktionen und legen sieben Evaluationsstufen fest, die das zunehmende Vertrauen in die Fähigkeit eines EVG widerspiegeln, seine Sicherheitsvorgaben zu erfüllen. Damit können diese Kriterien auf einen größeren Bereich von Systemen und Produkten angewendet werden als die TCSEC. Im allgemeinen hat ein EVG bei identischer Funktionalität und gleichwertiger Vertrauensstufe einen größeren Freiraum hinsichtlich seiner Architektur bei den ITSEC als bei den TCSEC, ist jedoch bezüglich der erlaubten Entwicklungsmethoden mehr eingeschränkt.

1.38 Als Beispiele wurden bestimmte Funktionalitätsklassen so definiert, daß sie weitgehend den Funktionalitätsanforderungen der TCSEC-Klassen C1 bis A1 entsprechen. Sie sind bei den Beispielen für Funktionalitätsklassen im Anhang 1 als F-C1 bis F-B3 aufgeführt. Es ist jedoch nicht möglich, die Evaluationsstufen direkt mit den Vertrauensstufen der TCSEC-Klassen zu vergleichen, weil die Stufen der ITSEC im Rahmen einer Harmonisierung von mehreren europäischen IT-Sicherheitskriterienkatalogen entwickelt wurden und in diesen Katalogen etliche Anforderungen enthalten sind, die in den TCSEC nicht explizit erscheinen.

1.39 Die beabsichtigte Korrespondenz zwischen den vorliegenden Kriterien und den TCSEC ist wie folgt:

Diese Kriterien		TCSEC-Klassen
E0	<--->	D
F-C1,E1	<--->	C1
F-C2,E2	<--->	C2
F-B1,E3	<--->	B1
F-B2,E4	<--->	B2
F-B3,E5	<--->	B3
F-B3,E6	<--->	A1

1.40 Es sollte beachtet werden, daß es keine Funktionalitätsklasse F-A1 gibt, weil die funktionalen Forderungen der TCSEC-Klasse A1 die gleichen sind, wie die der Klasse B3. Ein Produkt, das mit dem Ziel entwickelt wurde, mit Aussicht auf Erfolg sowohl gegen die ITSEC als auch gegen die TCSEC evaluiert zu werden und bei dem nachgewiesen wurde, daß es eine der Klassen oder Kombinationen in der obigen Tabelle erfüllt, sollte auch eine Evaluation gegen die anderen Kriterien der entsprechenden Klasse oder Kombination erfolgreich bestehen. Allerdings fordern die TCSEC bei C1, daß Ergebnisse der Tests beim Entwickler als Nachweis vorgelegt werden müssen. So würde eine [F-C1,E1] Evaluation nur dann einer C1-Evaluation entsprechen, wenn sich der Auftraggeber dazu entschlossen hätte, die optionale Forderung bei E1 zu erfüllen und vor Beginn der Evaluation die Dokumentation der Tests gegen die Sicherheitsvorgaben zum Nachweis der erforderlichen Tests zur Verfügung zu stellen.

1.41 In den TCSEC werden die sicherheitsspezifischen und sicherheitsrelevanten Funktionen des EVG zusammen als "*Trusted Computing Base*" (TCB) bezeichnet. Bei den höheren Klassen in den Gruppen B und A der TCSEC wird zusätzliches Vertrauen aus strengeren Anforderungen an die Architektur und die Konstruktion des TCB bezogen. Ab der TCSEC-Klasse B2 wird gefordert, daß die Zugriffsüberprüfung durch einen Zugriffsüberprüfungsmechanismus realisiert wird, der dem Konzept eines "Referenzmonitors" entspricht [AND]. Dieser Zugriffsüberprüfungsmechanismus muß untäuschbar sein, er muß immer aufgerufen werden und er muß klein genug sein, damit an ihm vollständige Analysen und Tests durchgeführt werden können.

1.42 Um mit den TCSEC kompatibel zu sein, schreiben die Beispiele der ITSEC-Funktionalitätsklassen F-B2 und F-B3 vor, daß die Zugriffskontrolle durch einen solchen Mechanismus realisiert wird. Zusätzlich fordern die ITSEC für höhere Evaluationsstufen Einschränkungen bezüglich der Architektur und der Konstruktion bei der Implementierung aller sicherheitsspezifischen Funktionen. Zusammen mit den ITSEC-Anforderungen zur Wirksamkeit, nämlich daß die sicherheitsspezifischen Funktionen geeignet sind und sich auch gegenseitig unterstützen, bedeutet dies: Ein EVG, der in der Lage sein soll, höhere Evaluationsstufen der ITSEC zu erfüllen und der über eine Funktionalität verfügt, die einer der TCSEC-Funktionalitätsklassen entspricht, muß zwingend die TCSEC-Forderungen nach einer TCB erfüllen und das Konzept des Referenzmonitors realisieren.

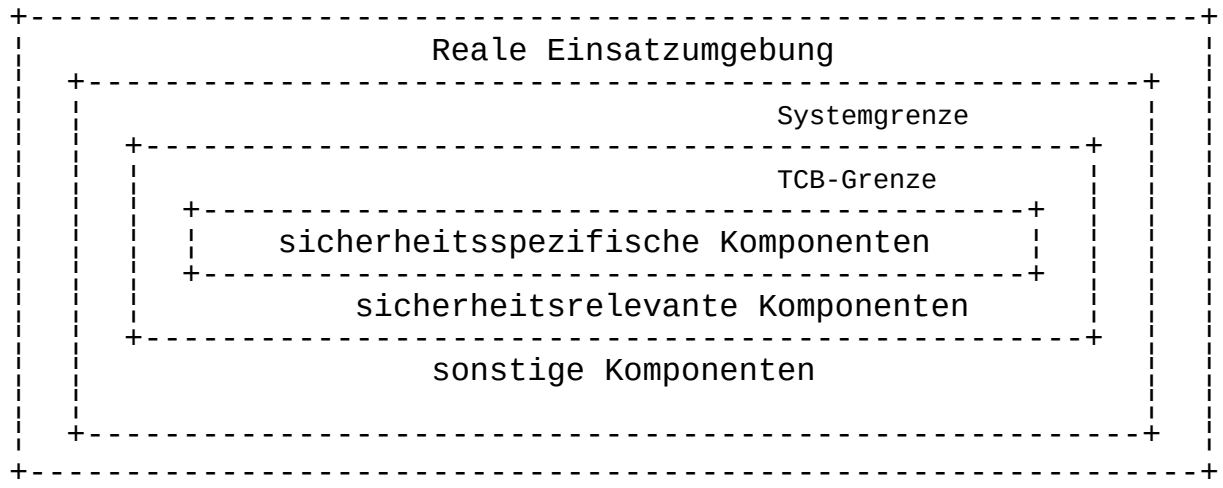


Abb. 1 IT-System

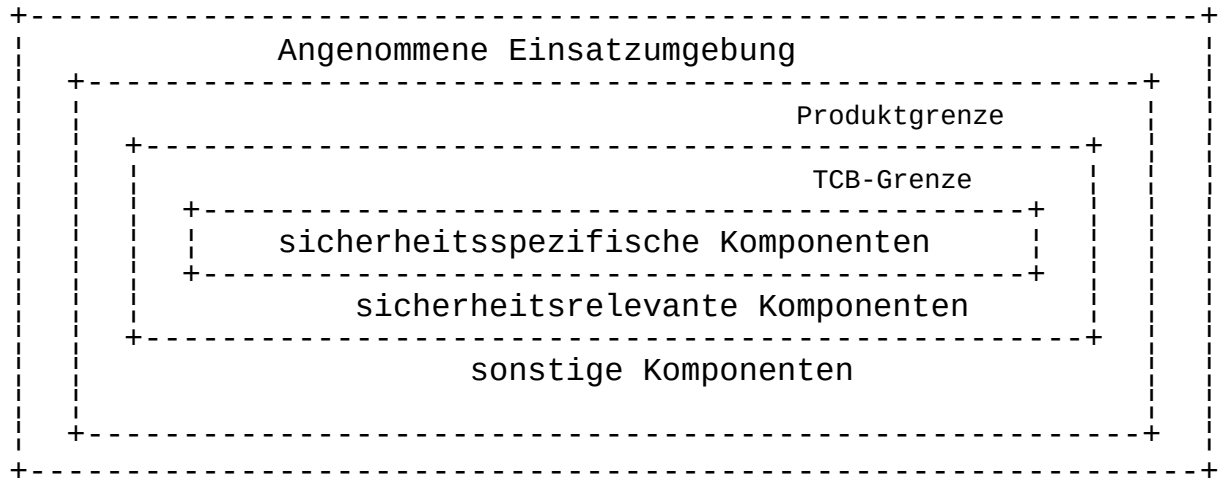


Abb. 2 IT-Produkt

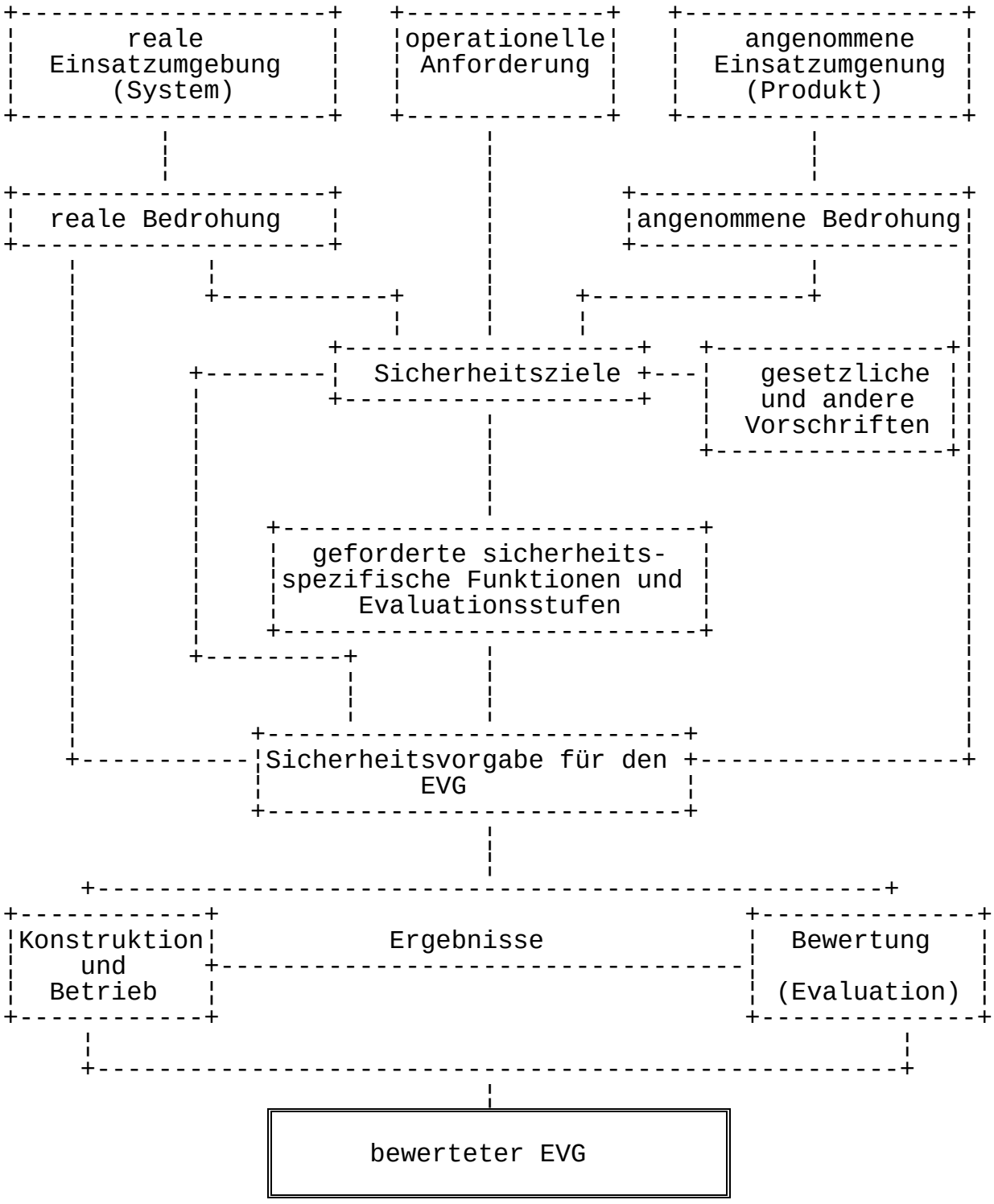


Abb. 3 Entwicklungs- und Bewertungsvorgang

2 FUNKTIONALITÄT

Einleitung

2.1 Ein Evaluationsgegenstand (EVG), der Sicherheit bietet (eine Kombination von Vertraulichkeit, Integrität und Verfügbarkeit) muß geeignete Sicherheitseigenschaften aufweisen. Normalerweise wird es notwendig sein, festzulegen, daß in diese Eigenschaften ein angemessener Grad von Vertrauen gesetzt werden kann. Damit dies möglich ist, müssen die Eigenschaften selbst beschrieben werden. Das Dokument oder die Dokumente, in dem bzw. in denen diese Eigenschaften beschrieben werden, stellen zusammen mit der angestrebten Evaluationsstufe die Sicherheitsvorgaben für den EVG dar.

2.2 In diesen Kriterien werden die Sicherheitsmaßnahmen auf drei Ebenen betrachtet. Die abstrakteste Betrachtungsweise ist die der Sicherheitsziele: der Beitrag, den ein EVG zur Sicherheit leisten soll. Um diese Ziele zu erreichen, muß der EVG bestimmte sicherheitsspezifische Funktionen enthalten. Diese sicherheitsspezifischen Funktionen müssen wiederum durch besondere Sicherheitsmechanismen realisiert werden. Diese drei Ebenen können wie folgt zusammengefaßt werden:

a) Sicherheitsziele - weshalb die Funktionalität gebraucht wird

b) Sicherheitsspezifische Funktionen - welche Funktionalität wirklich zur Verfügung gestellt wird

c) Sicherheitsmechanismen - wie die Funktionalität zur Verfügung gestellt wird

Die Sicherheitsvorgaben

2.3 Die Sicherheitsvorgaben dienen sowohl der Spezifikation der sicherheitsspezifischen Funktionen, gegen die der EVG evaluiert wird, als auch zur Beschreibung, wie die Einsatzumgebung des EVG beschaffen sein soll. Die Sicherheitsvorgaben sind deshalb nicht nur für die Personen gedacht, die für die Herstellung des EVG und seine Evaluation verantwortlich sind, sondern auch für die Personen, die für das Management, die Beschaffung, die Installation, die Konfiguration, den Betrieb und die Nutzung verantwortlich sind.

2.4 Der geforderte Inhalt der Sicherheitsvorgaben kann wie folgt zusammengefaßt werden:

a) *Entweder* eine **System-Sicherheitspolitik**
oder eine **Produktbeschreibung**.

b) Eine Spezifikation der geforderten sicherheitsspezifischen Funktionen.

c) Eine Definition geforderter Sicherheitsmechanismen *(optional)*.

d) Die postulierte Mindeststärke der Mechanismen.

e) Die angestrebte Evaluationsstufe.

Jeder dieser Punkte ist im folgenden genauer beschrieben.

2.5 Die Anforderungen an die Form der Sicherheitsvorgaben hängt von der angestrebten Evaluationsstufe ab. Die Evaluationsstufe bestimmt, welche Dokumentation über den EVG für eine Evaluation zur Verfügung gestellt werden muß, die Anforderungen an Inhalt und Form und die Anforderungen für den Nachweis, der vorgelegt werden muß, um zu zeigen, daß der EVG die Sicherheitsvorgaben erfüllt.

2.6 Die Sicherheitsvorgaben können als ein einziges Dokument oder in mehreren Dokumenten vorgelegt werden. Wenn mehrere Dokumente vorgelegt werden, muß der Zusammenhang zwischen ihnen klar aufgezeigt werden.

2.7 Der Antragsteller einer Evaluation ist für die Bereitstellung und Richtigkeit der Sicherheitsvorgaben für die Evaluation verantwortlich.

System-Sicherheitspolitik

2.8 Der Inhalt der Sicherheitsvorgaben hängt davon ab, ob es sich bei dem EVG um ein System oder um ein Produkt handelt. Im Falle eines Systems ist die Umgebung, in der der EVG eingesetzt wird, bekannt. Seine Sicherheitsziele können bestimmt und seine Bedrohungen und die vorhandenen Gegenmaßnahmen können berücksichtigt werden. Diese Angaben werden in der System-Sicherheitspolitik niedergelegt.

2.9 Die System-Sicherheitspolitik beschreibt die Gesetze, Regeln und Praktiken, die festlegen, wie sensitive Informationen und andere Betriebsmittel in einem bestimmten System verwaltet, geschützt und verteilt werden. Sie muß die Sicherheitsziele des Systems und die Bedrohungen gegen das System aufzeigen. Diese Sicherheitsziele müssen sowohl durch eine Kombination von sicherheitsspezifischen Funktionen im System (implementiert im EVG), als auch durch zugehörige materielle, personelle und organisatorische Maßnahmen erfüllt werden. Die System-Sicherheitspolitik muß alle Aspekte der Sicherheit beleuchten, die das System betreffen, einschließlich der zugehörigen materiellen, organisatorischen und personellen Sicherheitsmaßnahmen.

2.10 Jede Organisation wird in Zukunft über allgemeine Sicherheitstandards verfügen, die für alle Systeme innerhalb der Organisation gelten und die das Verhältnis zwischen der Organisation und der Außenwelt regeln. Diese Standards können als "**firmenspezifische Sicherheitspolitik**" bezeichnet werden, also als die Gesetze, Regeln und Praktiken, die festlegen wie Betriebsmittel, einschließlich der sensitiven Informationen, in der Organisation verwaltet, geschützt und verteilt werden. Viele Organisationen werden über eine explizit formulierte firmenspezifische Sicherheitspolitik verfügen, die die Regeln und Praktiken und die geltenden nationalen und internationalen Gesetze spezifiziert. Wo dies der Fall ist, soll in der System-Sicherheitspolitik darauf verwiesen

werden. Wenn nicht, müssen alle wichtigen Aspekte in jeder System-Sicherheitspolitik der Organisation aufgeführt werden.

2.11 Die primäre Hauptaufgabe der firmenspezifischen Sicherheitspolitik ist es, den Rahmen für die Festlegung der Sicherheitsziele des Systems zur Verfügung zu stellen. Die Aufzählung der wesentlichen Betriebsmittel der Firma, der allgemeinen Bedrohungen und der Ergebnisse der Risikoanalyse unterstützen die Festlegung der Sicherheitsziele des Systems. Wie eine Risikoanalyse durchgeführt wird, liegt außerhalb des Rahmens dieser Kriterien.

2.12 Für ein einzelnes System soll die System-Sicherheitspolitik die Sicherheitsmaßnahmen definieren, die eingesetzt werden, um die System-Sicherheitsziele so zu erfüllen, daß sie mit der firmenspezifischen Sicherheitspolitik übereinstimmen. Die Sicherheitsmaßnahmen, die durch die System-Sicherheitspolitik gefordert werden, werden durch eine Kombination von sicherheitsspezifischen Funktionen im EVG und durch materielle, personelle und organisatorische Maßnahmen realisiert. Die System-Sicherheitspolitik muß die Aufteilung der Verantwortlichkeit zwischen den sicherheitsspezifischen Funktionen und den anderen Maßnahmen klar aufzeigen.

2.13 Die IT-Sicherheitsmaßnahmen einer System-Sicherheitspolitik können vom Rest der System-Sicherheitspolitik getrennt werden und in einem besonderen Dokument festgelegt werden: der sogenannten "**Technischen Sicherheitspolitik**." Sie ist die Menge der Gesetze, Regeln und Praktiken, die die Verarbeitung von sensitiven Informationen und die Nutzung der Betriebsmittel durch die Hard- und Software eines IT-Systems regelt.

2.14 In vielen Fällen kann es sinnvoll sein, die Beschreibung der sicherheitsspezifischen Funktionen in die System-Sicherheitspolitik oder in die Technische Sicherheitspolitik einzubeziehen.

2.15 Die System-Sicherheitspolitik oder Technische Sicherheitspolitik kann als Grundlage für die Auswahl beim Kauf von IT-Sicherheitsprodukten benutzt werden; die Beschreibung einer solchen Produktauswahl liegt außerhalb des Rahmens dieser Kriterien.

Produktbeschreibung

2.16 Im Fall eines Produktes ist die genaue Umgebung, in der das Produkt eingesetzt werden wird, dem Entwickler nicht bekannt, da es in mehr als einem System oder in mehr als einer Systemumgebung eingesetzt werden kann. Stattdessen muß dem zukünftigen Anwender eine Beschreibung über das Produkt zur Verfügung gestellt werden, die ihm notwendige Informationen zur Verfügung stellt. Mit ihrer Hilfe soll er entscheiden können, ob das Produkt dazu beitragen kann, seine System-Sicherheitsziele zu erreichen, und festlegen können, was noch zusätzlich getan werden muß, damit diese Ziele vollständig erreicht werden.

2.17 Die Produktbeschreibung muß sowohl die vorgesehene Art der Nutzung des Produktes als auch die vorgesehene Einsatzumgebung und die angenommenen Bedrohungen beschreiben. Sie muß weiterhin eine Zusammenstellung der Sicherheitseigenschaften des Produktes enthalten und alle Annahmen über die Umgebung und die Art der Nutzung beschreiben. Darin müssen enthalten sein

- die personellen, materiellen, organisatorischen und IT-Sicherheitsmaßnahmen, die notwendig sind, um das Produkt einzusetzen;
- die Abhängigkeiten des Produkts von System-Hardware, Software und/oder Firmware, die nicht zum Lieferumfang des Produkts gehören.

Spezifikation der sicherheitsspezifischen Funktionen

2.18 Die Sicherheitsvorgaben müssen eine Spezifikation der sicherheitsspezifischen Funktionen enthalten, die vom EVG zur Verfügung gestellt werden. Diese Funktionen können entweder explizit oder durch Verweis auf eine oder mehrere vordefinierte Funktionalitätsklassen oder auf einen anerkannten Standard, der Sicherheitsfunktionalität definiert, angegeben werden. Vordefinierte Klassen werden später in diesem Kapitel behandelt.

2.19 Einer oder mehrere Standards, die sich auf Sicherheit beziehen, können Teil der Sicherheitsvorgaben sein, entweder durch Verweis oder durch explizite Angabe. Dort wo der Standard Wahlmöglichkeiten zulässt, müssen die ausgewählten Möglichkeiten klar angegeben werden. Wenn ein Standard nicht alle benötigten Informationen beinhaltet, müssen die notwendigen Informationen explizit in den Sicherheitsvorgaben ergänzt werden.

2.20 Bei Systemen müssen die sicherheitsspezifische Funktionen zu den Sicherheitszielen in Bezug gebracht werden, so daß erkennbar wird, durch welche Funktionen welche Ziele erreicht werden (eine Funktion kann zu mehr als einem Ziel beitragen). Jede Funktion in der Spezifikation der sicherheitsspezifischen Funktionen muß mindestens zu einem Ziel beitragen. Die Spezifikation der sicherheitsspezifischen Funktionen muß ebenfalls aufzeigen, warum die Funktionen dazu geeignet sind, die festgestellten oder angegebenen Bedrohungen der Sicherheitsziele abzuwehren.

2.21 Bei Produkten müssen die sicherheitsspezifischen Funktionen zu der vorgesehenen Art der Nutzung des Produktes und den Annahmen über die Einsatzumgebung des Produktes, die in der Produktbeschreibung angegeben sind, in Bezug gesetzt werden. Diese Korrelation muß alle Abhängigkeiten von anderen sicherheitsspezifischen Funktionen und von nicht-IT-Maßnahmen in der Einsatzumgebung enthalten.

2.22 Aus der Sicht der Evaluation ist die Spezifikation der sicherheitsspezifischen Funktionen der wichtigste Teil der Sicherheitsvorgaben. Diese Funktionen müssen immer informell in Umgangssprache beschrieben werden. Zusätzlich müssen sie bei höheren Evaluationsstufen in einer semiformalen oder formalen Darstellungsform spezifiziert werden. Solche Darstellungformen werden später in diesem Kapitel detaillierter behandelt.

Definition der geforderten Sicherheitsmechanismen

2.23 Die Sicherheitsvorgaben können optional die Benutzung eines besonderen Sicherheitsmechanismus vorschreiben oder fordern. Alle Sicherheitsmechanismen, die in den Sicherheitsvorgaben enthalten sind, müssen zu den entsprechenden sicherheitsspezifischen Funktionen in Bezug gesetzt werden, so daß erkannt werden kann, mit welchen Mechanismen welche Funktionen realisiert werden (ein Mechanismus kann mehrere Funktionen realisieren und eine Funktion kann durch eine Kombination von mehreren Mechanismen realisiert werden).

2.24 Wenn Sicherheitsmechanismen durch die Sicherheitsvorgaben vorgeschrieben werden, ist es Aufgabe des Entwicklers, die geforderten Mechanismen einzusetzen. Andernfalls gehört es zu den Aufgaben des Entwicklers des EVG, Mechanismen zu entwickeln und zu realisieren, die zusammen die geforderten sicherheitsspezifischen Funktionen bieten.

Angestrebte Mindeststärke von Mechanismen

2.25 In allen Sicherheitsvorgaben muß die angestrebte Mindeststärke der Sicherheitsmechanismen des EVG gegen direkten Angriff festgelegt werden. Die dafür vorgesehenen Stufen *niedrig*, *mittel* oder *hoch* sind im Kapitel 3 dieser Kriterien definiert.

Angestrebte Evaluationsstufe

2.26 In allen Sicherheitsvorgaben muß eine Evaluationsstufe als Vorgabe für die Evaluation des EVG festgelegt werden. Dies muß eine der Stufen *E1, E2, E3, E4, E5* oder *E6* sein. Diese Stufen sind im Kapitel 4 dieser Kriterien beschrieben.

Beispiele für die Nutzung von vorhandenen Sicherheitspolitik-Dokumenten

2.27 Die vorliegenden Kriterien erlauben es, vorhandene IT-Sicherheitspolitik-Dokumente, die nach anderen Kriterien oder Standards entwickelt wurden, entweder als Teil oder vollständig in den Sicherheitsvorgaben eines Systems zu nutzen. Aus diesem Grunde ist der genaue Inhalt der Dokumente, die die Sicherheitsvorgaben ausmachen, nicht vorgeschrieben. Die Angaben, die mindestens für eine Evaluation gegen diese Kriterien erforderlich sind, sind oben beschrieben. Da die Sicherheitsvorgaben aus mehr als einem Dokument bestehen können, können vorhandene Typen von Sicherheitspolitik-Dokumenten übernommen werden (obwohl zusätzliche Dokumente erforderlich sein können, um die Informationen zu vervollständigen, die für die Sicherheitsvorgaben notwendig sind).

2.28 Im folgenden wird anhand von zwei Beispielen gezeigt, wie spezielle Typen von Sicherheitspolitik-Dokumenten die Forderungen der Sicherheitsvorgaben erfüllen können.

2.29 In Großbritannien ist für alle Systeme, die nach dem nationalen Geheimschutz eingestufte Informationen verarbeiten, eine System-Sicherheitspolitik (System Security Policy, SSP) zwingend vorgeschrieben. Wenn die für die Genehmigung zuständige Dienststelle entscheidet, daß eine Bewertung der Sicherheit notwendig ist, muß ebenfalls

eine IT-Sicherheitspolitik (System Electronic Information Security Policy, SEISP) erstellt werden. Für bestimmte Evaluationsstufen muß ebenfalls ein Sicherheitsmodell (Security Policy Model, SPM) erstellt werden. Die SSP beschreibt die Aufgabe des Systems, seine Sicherheitsziele, die erforderlichen Sicherheitsmaßnahmen und die Festlegung der Verantwortung für ihre Durchführung (d.h. die SSP stimmt weitgehend mit der System-Sicherheitspolitik, die in diesen Kriterien beschrieben ist, überein). Sie enthält ebenfalls die Ableitung der angestrebten Evaluationsstufe auf der Grundlage von wesentlichen Eigenschaften des Systems und seiner Einsatzumgebung. Wenn notwendig, wird eine SEISP aus einer SSP entwickelt. Dies ist eine genauere Beschreibung der Hard- und Softwaresicherheitsaspekte aus der SSP, aber immer noch in einer informellen Darstellung: sie entspricht damit einer "technischen Sicherheitspolitik", die in diesen Kriterien beschrieben ist. Das Sicherheitsmodell ist eine weitere Spezifikation der sicherheitsspezifischen Funktionen einer SEISP in einer formalen oder halbformalen Darstellung. Es wird erstellt, wenn eine solche zweite Spezifikation für die angestrebte Evaluationsstufe gefordert ist.

2.30 Ein "Claims-Dokument" ist eine Liste von Aussagen über die sicherheitsspezifische Funktionalität, die ein Produkt angeblich bereitstellt. Es wird durch den Entwickler erstellt und halbformal unter Verwendung der im Anhang B dieses Dokumentes beschriebenen Sprache formuliert. Es enthält Annahmen darüber, wie das Produkt eingesetzt werden muß, damit diese Aussagen gelten. Damit das "Claims-Dokument" die Sicherheitsvorgaben für ein Produkt vollständig so abdeckt, wie es in diesen Kriterien gefordert wird, schließt es ebenfalls eine Beschreibung der Sicherheitsziele und eine informelle Spezifikation der sicherheitsspezifischen Funktionen ("Claims") mit ein. Außerdem muß es einen Bezug zwischen den sicherheitsspezifischen Funktionen und den Sicherheitszielen herstellen und die gewünschte Evaluationsstufe nennen.

Generische Oberbegriffe

2.31 Die Sicherheitsvorgaben sind einfacher zu verstehen, wenn die Spezifikation der sicherheitsspezifischen Funktionen in einer vernünftigen Ordnung dargestellt wurde. Dies hilft beim Vergleich unterschiedlicher Sicherheitsvorgaben und vereinfacht die Arbeit der Evaluatoren. Es gibt eine natürliche Einteilung der sicherheitsspezifischen Funktionen, aus denen sich eine solche Ordnung ableiten läßt. Acht *generische Oberbegriffe* für eine solche Einteilung werden in diesen Kriterien vorgeschlagen und beschrieben.

2.32 Die vorgeschlagenen Oberbegriffe sind:

Identifizierung und Authentisierung
Zugriffskontrolle
Beweissicherung
Protokollauswertung
Wiederaufbereitung
Unverfälschtheit
Zuverlässigkeit der Dienstleistung
Übertragungssicherung

2.33 Es wird empfohlen, möglichst diese Oberbegriffe zu benutzen. Ihr Gebrauch wird den Vergleich mit anderen Sicherheitsvorgaben vereinfachen und die Feststellung erleichtern, ob sicherheitsspezifische Funktionen eines bestimmten Typs in speziellen Sicherheitsvorgaben enthalten sind.

Identifizierung und Authentisierung

2.34 In vielen EVG wird es Anforderungen geben, diejenigen Benutzer zu bestimmen und zu überwachen, die Zugriff auf Betriebsmittel haben, die vom EVG kontrolliert werden. Dazu muß nicht nur die behauptete Identität des Benutzers festgestellt, sondern auch die Tatsache nachgeprüft werden, daß der Benutzer tatsächlich die Person ist, die er zu sein vorgibt. Dies geschieht, indem der Benutzer dem EVG Informationen liefert, die fest mit dem betreffenden Benutzer verknüpft sind.

2.35 Unter diesem Oberbegriff müssen alle Funktionen abgedeckt werden, die dazu dienen, die behauptete Identität zu bestimmen und nachzuprüfen.

2.36 Unter diesen Oberbegriff fallen auch alle Funktionen, durch die neue Benutzeridentitäten hinzugefügt und alte herausgenommen oder ungültig gemacht werden können. Desgleichen fallen darunter Funktionen, mit denen die Authentisierungsinformationen, die zur Nachprüfung der Identität bestimmter Benutzer nötig sind, erzeugt, geändert oder vom autorisierten Benutzer erfahren werden können. Funktionen, die die Integrität der Authentisierungsinformationen gewährleisten oder ihre unbefugte Verwendung verhindern, müssen ebenfalls hier behandelt werden. Unter diesem Oberbegriff müssen außerdem alle Funktionen behandelt werden, die die Möglichkeit begrenzen, wiederholt Versuche zum Erlangen einer falschen Identität zu machen.

Zugriffskontrolle

2.37 Bei vielen EVG wird es erforderlich sein, sicherzustellen, daß Benutzer und Prozesse, die für diese Benutzer tätig sind, daran gehindert werden, Zugriff auf Informationen oder Betriebsmittel zu erhalten, für die sie kein Zugriffsrecht haben oder für die keine Notwendigkeit zu einem Zugriff besteht. Desgleichen wird es Anforderungen bezüglich der unbefugten Erzeugung oder Änderung (einschließlich Löschung) von Informationen geben.

2.38 Unter diesem Oberbegriff müssen diejenigen Funktionen behandelt werden, die für die Kontrolle

- des Informationsflusses zwischen Benutzern, Prozessen und Objekten,
- der Betriebsmittelnutzung durch Benutzer, Prozesse und Objekte

vorgesehen sind. Das schließt die Verwaltung (z.B. Vergabe und Zurücknahme) von Zugriffsrechten und ihre Prüfung ein.

2.39 Unter diesem Oberbegriff müssen alle Funktionen für die Erstellung und Fortschreibung von Listen oder Regeln zusammengefaßt werden, durch die die Rechte zur Durchführung verschiedenartiger Zugriffe geregelt werden. Ebenso müssen darunter auch solche Funktionen fallen, die die zeitweiligen Einschränkungen des Zugriffs auf Objekte betreffen, auf die mehrere Benutzer oder Prozesse gleichzeitig Zugriff haben, und die erforderlich sind, um die Konsistenz und Unverfälschtheit solcher Objekte auf-

rechtzuerhalten. Unter diesem Oberbegriff müssen außerdem alle Funktionen behandelt werden, die sicherstellen, daß Objekte bei ihrer Erzeugung voreingestellten Zugriffslisten oder -regeln zugeordnet werden. Darunter fallen Funktionen, die die Weitergabe von Zugriffsrechten auf Objekte kontrollieren. Des weiteren müssen hier alle Funktionen beschrieben werden, mit denen eine Ableitung von Informationen überwacht werden kann, die durch Zusammenfügen von legitim zugänglichen Daten möglich ist.

Beweissicherung

2.40 Bei vielen EVG wird es erforderlich sein, sicherzustellen, daß über Handlungen, die von Benutzern bzw. von Prozessen im Namen solcher Benutzer ausgeführt werden, Informationen aufgezeichnet werden, damit die Folgen solcher Handlungen später dem betreffenden Benutzer zugeordnet werden können und der Benutzer für seine Handlungen verantwortlich gemacht werden kann.

2.41 Dieser Oberbegriff muß alle Funktionen abdecken, die dazu vorgesehen sind, die Ausübung von Rechten aufzuzeichnen, die für die Sicherheit von Bedeutung sind.

2.42 Unter diesem Oberbegriff müssen Funktionen behandelt werden, die sich auf die Erfassung, den Schutz und die Analyse solcher Informationen beziehen. Gewisse Funktionen können bestimmte Anforderungen sowohl der Beweissicherung als auch der Protokollauswertung erfüllen und somit für beide Oberbegriffe relevant sein. Solche Funktionen können unter jedem der beiden Oberbegriffe beschrieben werden, aber ein Verweis zu dem anderen Oberbegriff ist erforderlich.

Protokollauswertung

2.43 Bei vielen EVG wird sicherzustellen sein, daß sowohl über gewöhnliche Vorgänge als auch über außergewöhnliche Vorfälle ausreichend Informationen aufgezeichnet werden, damit durch Nachprüfungen später festgestellt werden kann, ob tatsächlich Sicherheitsverletzungen vorgelegen haben und welche Informationen oder sonstigen Betriebsmittel davon betroffen waren.

2.44 Dieser Oberbegriff muß alle Funktionen umfassen, die zur Auffindung und Überprüfung von Ereignissen vorgesehen sind, die eine Bedrohung für die Sicherheit darstellen könnten.

2.45 Dieser Oberbegriff muß Funktionen zur Erfassung, zum Schutz und zur Analyse solcher Informationen enthalten. Eine solche Analyse kann auch eine Trendanalyse einschließen, die dazu benutzt wird, potentielle Verletzungen der Sicherheitsvorgaben zu entdecken, bevor eine solche Verletzung stattfindet. Gewisse Funktionen können bestimmte Anforderungen sowohl der Beweissicherung als auch der Protokollauswertung erfüllen und somit für beide Oberbegriffe relevant sein. Diese Funktionen können unter jedem der beiden Oberbegriffe beschrieben werden, aber ein Verweis zu dem anderen Oberbegriff ist erforderlich.

Wiederaufbereitung

2.46 Bei vielen EVG wird es erforderlich sein, sicherzustellen, daß Betriebsmittel wie beispielsweise Hauptspeicher oder Bereiche von Plattenspeichern unter Aufrechterhaltung

der Sicherheit wiederverwendet werden können.

2.47 Dieser Oberbegriff muß alle Funktionen umfassen, die für die Überwachung der Wiederaufbereitung von Datenobjekten vorgesehen sind.

2.48 Der Oberbegriff muß auch Funktionen zum Initialisieren oder zum Löschen nicht oder wieder zugeordneter Datenobjekte enthalten. Er muß Funktionen enthalten, um wiederverwendbare Medien, wie z.B. Magnetbänder, zu initialisieren bzw. ihren Inhalt zu löschen oder um Ausgaben auf Ausgabegeräten, wie z.B. Bildschirmen, zu löschen, wenn diese nicht in Betrieb sind.

Unverfälschtheit

2.49 Bei vielen EVG wird es erforderlich sein, sicherzustellen, daß bestimmte Beziehungen zwischen unterschiedlichen Daten korrekt bleiben und daß Daten zwischen einzelnen Prozessen ohne Änderungen übertragen werden.

2.50 Dieser Oberbegriff muß alle Funktionen umfassen, die sicherstellen, daß Daten nicht in unbefugter Weise geändert wurden.

2.51 Dieser Oberbegriff muß Funktionen zur Bestimmung, Einrichtung und Aufrechterhaltung der Unverfälschtheit der Beziehungen zwischen zusammenhängenden Daten enthalten. Daneben müssen auch Funktionen bereitgestellt werden, die es bei der Übertragung von Daten zwischen einzelnen Prozessen, Benutzern und Objekten ermöglichen, Verluste, Ergänzungen oder Veränderungen zu entdecken bzw. zu verhindern, und die es unmöglich machen, die angebliche oder tatsächliche Herkunft bzw. Bestimmung der Datenübertragung zu ändern.

Zuverlässigkeit der Dienstleistung

2.52 Bei vielen EVG wird es erforderlich sein, sicherzustellen, daß zeitkritische Aufgaben genau zu dem Zeitpunkt durchgeführt werden müssen, zu dem es erforderlich ist, also nicht früher oder später, und es wird sicherzustellen sein, daß zeitunkritische Aufgaben nicht in zeitkritische umgewandelt werden können. Desgleichen wird es bei vielen EVG erforderlich sein, sicherzustellen, daß ein Zugriff in dem erforderlichen Moment möglich ist und Betriebsmittel nicht unnötig angefordert oder zurückgehalten werden.

2.53 Dieser Oberbegriff muß alle Funktionen umfassen, die dafür sorgen, daß auf Anforderung einer autorisierten Stelle (z.B. ein Nutzer oder ein Prozeß, der einen Nutzerauftrag ausführt) die Betriebsmittel zugänglich und benutzbar sind, und die die Beeinflussung von zeitkritischen Operationen verhindern oder einschränken.

2.54 Unter diesen Oberbegriff müssen Funktionen für die Fehlerentdeckung und -überbrückung fallen, die die Auswirkungen von Fehlern auf den Betrieb des EVG begrenzen und dadurch Unterbrechungen oder Leistungsverluste minimieren. Es müssen hier ebenfalls alle Steuerungsfunktionen einbezogen werden, die sicherstellen, daß der EVG auf externe Anforderungen reagiert und Ausgaben innerhalb festgelegter Zeiten zur Verfügung stellt.

Übertragungssicherung

2.55 In vielen EVG wird es Anforderungen zum Schutz der Daten während ihrer Übertragung über Kommunikationskanäle geben. Dies wird normalerweise mit Fernmeldesicherheit bezeichnet, im Unterschied zur DV(IT)-Sicherheit.

2.56 Dieser Oberbegriff muß alle Funktionen umfassen, die für den Schutz der Daten während der Übertragung über Kommunikationskanäle vorgesehen sind. Es wird empfohlen, solche Funktionen mit folgenden Unterbegriffen zu beschreiben, die aus der OSI-Sicherheitsarchitektur stammen:

Authentisierung
Zugriffskontrolle
Datenvertraulichkeit
Datenintegrität
Sende- und Empfangsnachweis

2.57 Funktionen müssen nach diesen Unterbegriffen in einer Weise gegliedert werden, die mit ihrer Nutzung und der Definition in der OSI-Sicherheitsarchitektur [OSI] übereinstimmt.

2.58 Gewisse Funktionen erfüllen möglicherweise sowohl die Forderungen der Fernmelde- als auch der DV-Sicherheit und sind so für andere Oberbegriffe von Bedeutung. In diesen Fällen ist ein Verweis zu den anderen betroffenen Oberbegriffen erforderlich.

Vordefinierte Klassen

2.59 Viele Systeme werden ähnliche Sicherheitsziele haben; es wird häufig möglich sein, gemeinsame Mengen von sicherheitsspezifischen Funktionen zu identifizieren, die diese Ziele erfüllen. Ebenso werden viele Sicherheitsprodukte darauf ausgerichtet sein, die gleichen Forderungen des Marktes zu erfüllen, und besitzen damit eine ähnliche Funktionalität. Solche *vordefinierten Klassen* von gemeinsamen Funktionen können als Grundlage für bestimmte System- oder Produkt-Sicherheitsvorgaben benutzt werden oder sie können als Richtlinien benutzt werden, um Anwendern bei der Auswahl der passenden Sicherheitsfunktionalität zu helfen, damit ihre besonderen Sicherheitsziele erreicht werden, und um Herstellern bei der Auswahl der Funktionen zu helfen, die sie in ihre Produkte aufnehmen. Um den größtmöglichen Nutzen aus einer solchen Gemeinsamkeit zu ziehen, ist es wünschenswert, daß Standards für vordefinierte Funktionalitätsklassen vorhanden sind. Die vorliegenden Kriterien lassen deshalb in den Sicherheitsvorgaben einen Verweis auf vordefinierte Klassen von sicherheitsspezifischen Funktionen zu. In Sicherheitsvorgaben kann auf eine oder mehrere vordefinierte Klasse(n) verwiesen werden, um Teile oder die Gesamtheit der sicherheitsspezifischen Funktionen festzulegen.

2.60 Organisationen für die Standardisierung oder solche, die einen besonderen Sektor des Marktes repräsentieren, haben bereits solche Standarddefinitionen entwickelt. Es wird angenommen, daß die Verfügbarkeit der vorliegenden Kriterien die Entwicklung von

weiteren vordefinierten Klassen fördern wird, die mit der Anwendung dieser Kriterien verträglich ist. Da sich die IT-Sicherheit jedoch schnell weiterentwickeln wird, ist es notwendig, zukünftig weitere vordefinierte Klassen festzulegen, sobald neue Gruppen von Funktionen genügend weit anerkannt sind und als sinnvoll betrachtet werden.

2.61 Genauso, wie für jede vordefinierte Klasse ihre sicherheitsspezifischen Funktionen spezifiziert werden, muß das Ziel jeder Klasse, ihre beabsichtigte Anwendung und die Gründe für die Auswahl bestimmter Funktionen angegeben werden. Vordefinierte Klassen können auch andere Informationen enthalten, die für eine Aufnahme in die Sicherheitsvorgaben notwendig sind, wie z.B. Einzelheiten über Mechanismen, die für diese Klasse vorgeschrieben sind. Unter der Voraussetzung, daß der Inhalt solcher Klassen öffentlich verfügbar ist, müssen Details nicht in allen Sicherheitsvorgaben wiederholt werden, die auf Klassen verweisen.

2.62 Die Anwendung von vordefinierten Klassen ist nicht zwingend. Es wird Fälle geben, in denen der Antragsteller einer Evaluation sie nicht anwenden will, und Fälle, in denen sie nicht angewendet werden können, z.B. weil keine vordefinierte Klasse die gewünschten Sicherheitseigenschaften beschreibt. Als Alternative zu den vordefinierten Klassen können die sicherheitsspezifischen Funktionen immer individuell spezifiziert werden. Eine Beschreibung individueller Funktionen kann zusammen mit einer oder mehreren vordefinierten Klasse(n) in den Sicherheitsvorgaben verwendet werden. Jedoch darf eine vordefinierte Klasse nur dann als Teil von Sicherheitsvorgaben spezifiziert werden, wenn alle Aspekte dieser Klasse sich in den Sicherheitsvorgaben wiederfinden.

2.63 Zehn Beispiele für vordefinierte Klassen werden in Anhang A beschrieben. Sie wurden aus den Funktionalitätsklassen abgeleitet, die in [ZSIEC] beschrieben sind. Alle werden in einer informellen Weise dargestellt und sind in der gegenwärtigen Version der ITSEC lediglich vorläufig. Es sind:

a) Die exemplarischen Funktionalitätsklassen F-C1, F-C2, F-B1, F-B2 und F-B3 sind hierarchisch geordnete Klassen der Vertraulichkeit, die eng den Funktionalitätsanforderungen der TCSEC-Klassen C1 bis A1 [TCSEC] entsprechen.

b) Die exemplarische Funktionalitätsklasse F-IN gilt für EVG mit hohen Integritätsanforderungen an Daten und Programme. Anforderungen dieser Art sind z.B. bei Datenbanken von Bedeutung.

c) Die exemplarische Funktionalitätsklasse F-AV stellt hohe Anforderungen an die Verfügbarkeit eines gesamten EVG oder spezieller Funktionen eines EVG. Solche Forderungen sind zum Beispiel bei Prozeßsteuerungssystemen wichtig.

d) Die exemplarische Funktionalitätsklasse F-DI stellt hohe Anforderungen an die Wahrung der Datenintegrität während der Datenübertragung.

e) Die exemplarische Funktionalitätsklasse F-DC ist vorgesehen für EVG mit hohen Ansprüchen an die Vertraulichkeit von Daten während der Datenübertragung. Ein Beispiel für diese Klasse sind Kryptogeräte.

f) Die exemplarische Funktionalitätsklasse F-DX ist für Netze vorgesehen, bei denen hohe Ansprüche an die Vertraulichkeit und Integrität der zu übertragenden Informationen gestellt werden. Dies kann beispielsweise der Fall sein, wenn sensitive Informationen über unsichere (z.B. öffentliche) Netze zu übertragen sind.

2.64 Es gibt keine Einschränkung für die spezifische Funktionalität, die in den Sicherheitsvorgaben postuliert oder gefordert werden kann. Die sicherheitsspezifischen Funktionen in Sicherheitsvorgaben können mit den verfügbaren Darstellungsmitteln für Spezifikationen vollständig beschrieben werden. Das Vorhandensein einer vordefinierten Klasse schränkt Hersteller bei der Weiterentwicklung der Technik nicht ein; eher wird dadurch der Aufwand für die Spezifikation von Systemen verringert, die den beschriebenen Stereotypen gleichen, und es wird eine Grundlage für den Vergleich der angebotenen Funktionalität geboten. Sicherheitsvorgaben für Produkte können, selbst wenn eine Übereinstimmung mit einer vordefinierten Klasse postuliert wird, zusätzliche Einschränkungen und Anforderungen an die Einsatzumgebung festlegen, damit mögliche Nutzer beurteilen können, ob das Produkt für ihre spezielle Einsatzumgebung geeignet ist.

Spezifikationsformen

2.65 Die vorliegenden Kriterien schreiben keine Anwendung von anwendereigenen oder standardisierten Methoden oder Darstellungsformen für die Spezifikation von sicherheitsspezifischen Funktionen vor. Es werden auch keine Methoden oder Darstellungsformen ausgeschlossen, solange die Anforderungen der angestrebten Evaluationsstufe bezüglich der Form und des Nachweises erfüllt werden. Damit mögliche Ansätze für die Spezifikation kategorisiert werden können, werden drei Darstellungsformen in diesen Kriterien unterschieden: informell, halbformal und formal. Jede dieser Darstellungsformen wird im folgenden näher beschrieben.

2.66 Nicht alle Personen, die sich mit Sicherheitsvorgaben beschäftigen müssen, sind in der Lage, Spezifikationen in halbformaler oder formaler Form zu verstehen. Deshalb müssen alle Sicherheitsvorgaben eine Spezifikation der sicherheitsspezifischen Funktionen in einer informellen Form enthalten. Obgleich das Verständnis informeller Spezifikationen keine besondere Ausbildung voraussetzt, sind sie oft mehrdeutig und ungenau. Semiformale und formale Spezifikationen verringern die Möglichkeit der Mehrdeutigkeit und der Ungenauigkeit. Aus diesem Grunde muß für die höheren Evaluationsstufen die informelle Spezifikation der sicherheitsspezifischen Funktionen durch eine zugehörige semiformale oder formale Spezifikation ergänzt werden.

2.67 Die Darstellungsform, die für die Beschreibung der Sicherheitsziele oder von vorgeschriebenen oder vorhandenen Sicherheitsmechanismen in den Sicherheitsvorgaben benutzt wird, liegt außerhalb des Rahmens dieser Kriterien.

2.68 Wenn von Sicherheitsvorgaben gefordert wird, daß sie eine Spezifikation der sicherheitsspezifischen Funktionen in einer besonderen Form enthalten, kann diese Spezifikation ganz oder teilweise durch einen Hinweis auf eine oder mehrere vordefinierte Klassen ersetzt werden, die in einer solchen Form geschrieben sind.

2.69 Unabhängig von der Form kann eine geforderte Spezifikation als ein einzelnes Dokument oder in mehreren Dokumenten vorgelegt werden. Werden mehrere Dokumente vorgelegt, so muß der Zusammenhang zwischen ihnen klar aufgezeigt werden.

Informelle Spezifikation

2.70 Eine informelle Spezifikation ist in Umgangssprache geschrieben und nicht in einer Form, die besonderen Einschränkungen oder Konventionen unterliegt. Als Umgangssprache bezeichnet man die Kommunikation in jeder üblicherweise gesprochenen Sprache (z.B. Holländisch, Englisch, Französisch, Deutsch). Spezifikationen in Umgangssprache unterliegen keinen speziellen Einschränkungen, sie müssen allerdings den üblichen Konventionen der Sprache entsprechen (z.B. Grammatik und Syntax).

2.71 Eine Spezifikation in Umgangssprache muß mit dem Ziel geschrieben werden, Mehrdeutigkeiten zu vermeiden, indem alle Ausdrücke in einheitlicher Weise benutzt werden und Ausdrücke mit besonderer Bedeutung (einer Bedeutung, die nicht in einem gängigen Wörterbuch enthalten ist) in einem Glossar oder mehreren Glossaren definiert werden, das der Spezifikation beigefügt ist oder auf das verwiesen wird. Wahrscheinlich lassen sich Mehrdeutigkeiten nicht vollständig ausschalten. Während einer Evaluation wird man versuchen, verbliebene Mehrdeutigkeiten herauszufinden und zu klären.

Semiformale Spezifikation

2.72 Eine semiformale Darstellungsform einer Spezifikation erfordert die Benutzung einer eingeschränkten Notation (oder Notationen) unter Einhaltung bestimmter Konventionen, die Teil der Spezifikation sind oder auf die in der Spezifikation verwiesen wird. Diese Konventionen werden informell beschrieben. Eine solche Notation muß sowohl die Beschreibung der Wirkung jeder Funktion als auch die Beschreibung aller damit zusammenhängenden Ausnahmen und Fehler erlauben.

2.73 Eine semiformale Spezifikation kann entweder eine graphische Darstellung sein oder sie kann auf einer eingeschränkten Nutzung der Umgangssprache aufgebaut sein (z.B. eingeschränkte Satzstruktur und Schlüsselworte mit spezieller Bedeutung). Beispiele für halbformale Formen sind Datenflußdiagramme, Zustandsübergangsdiagramme, Entity-Relationship-Diagramme, Datenstrukturdiagramme, Prozeß- oder Programmstrukturdiagramme und die vom CCITT empfohlene Spezifikationssprache SDL.

2.74 Strukturierte Entwurfs- und Entwicklungsmethoden beinhalten normalerweise mindestens eine dieser semiformalen Notationen zur Sammlung der Anforderungen und daneben Hinweise (z.B. Maße für die Komplexität und Methoden für das Management) zur Nutzung dieser Notation. Beispiele für strukturierte Entwurfsmethoden, die solche Notationen enthalten, sind: Yourdon Structured Method [YSM], Structured Analysis and Design Technique [SADT], Structured Systems Analysis and Design Method [SSADM], Jackson Structured Design [JSD] und Jackson Structured Programming [JSP] Methods.

2.75 Ein besonderes Beispiel einer semiformalen Schreibweise, die erfolgreich bei der Erstellung von Sicherheitsvorgaben eingesetzt wurde, ist die "Claims"-Sprache. Die "Claims"-Sprache ist eine Teilmenge der Englischen Sprache; sowohl Vokabular als auch Grammatik der Sätze sind eingeschränkt. Sie wurde (wie der Name anzeigt) entwickelt, um Aussagen über die Sicherheitseigenschaften von IT-Produkten auf eine strukturierte Weise formulieren zu können. Die "Claims"-Sprache erlaubt es, vorhandene sicherheitsspezifische Funktionen in Umgangssprache als Teil der Sicherheitsvorgaben zu beschreiben. Anhang B enthält zur Erläuterung der Struktur eine formale Übersetzung der "Claims"-Sprache. Das englische Original ist mit den ITSEC Kriterien vereinbar.

Formale Spezifikation

2.76 Eine formale Darstellungsform einer Spezifikation ist in einer formalen Notation geschrieben, die auf wohl begründeten mathematischen Konzepten aufbaut. Diese Konzepte werden dazu benutzt, um die Syntax und die Semantik der Notation und die Prüfregeln zu definieren, die das logische Schließen unterstützen. Formale Spezifikationen müssen aus einer Menge von Axiomen abgeleitet werden können. Die Gültigkeit von Haupteigenschaften, wie z.B. die Erzeugung einer gültigen Ausgabe für alle Eingaben, muß gezeigt werden können. Wenn Spezifikationen hierarchisch aufgebaut sind, muß gezeigt werden können, daß auf jeder Stufe die Eigenschaften der vorhergehenden Stufe erhalten bleiben.

2.77 Die syntaktischen und semantischen Regeln einer formalen Notation, die in Sicherheitsvorgaben verwendet werden, müssen festlegen, wie Konstrukte eindeutig zu erkennen sind und ihre Bedeutung bestimmt werden kann. Wenn Beweisregeln logische Schlüsse unterstützen, muß offensichtlich sein, daß es nicht möglich ist, Widersprüche abzuleiten. Alle Regeln der Notation müssen definiert werden oder es muß darauf hingewiesen werden, wo sie beschrieben sind. Alle Konstrukte, die in einer formalen Spezifikation benutzt werden, müssen vollständig durch die Regeln beschrieben sein. Die formale Notation muß sowohl die Beschreibung der Wirkung einer Funktion als auch aller damit zusammenhängenden Ausnahmen und Fehler erlauben.

2.78 Beispiele für formale Schreibweisen sind VDM, beschrieben in [SSVDM], Z, beschrieben in [ZRM], die Spezifikationssprache RAISE, beschrieben in [RSL], Ina Jo, beschrieben in [IJRM], die Spezifikationssprache Gipsy, beschrieben in [GIPSY] und die OSI-Sprache zur Spezifikation von Protokollen [LOTOS]. Die Nutzung von Konstrukten der Prädikaten- (oder anderer) Logik und der Mengenlehre als formale

Schreibweise ist erlaubt, wenn die Konventionen (Regeln) dokumentiert sind oder ein Verweis auf die Beschreibung (wie bereits oben erwähnt) angegeben ist.

Konsistenz von parallelen Spezifikationen in unterschiedlichen Darstellungsformen

2.79 Parallele Spezifikationen müssen so dargestellt werden, daß die Beziehungen zwischen den Spezifikationen klar sind und gleiche Themen in verschiedenen Spezifikationen konsistent behandelt werden. Parallele Spezifikationen können entweder als getrennte Dokumente vorgelegt werden oder sie können in einem einzigen Dokument zusammengefaßt werden.

2.80 Dort wo in einer informellen Spezifikation Mehrdeutigkeiten auftreten, muß die zugehörige formale oder halbformale Spezifikation diese Mehrdeutigkeit beseitigen. Es ist jedoch ein Fehler, wenn parallele Spezifikationen inkonsistent sind. Jeder solche Fehler muß durch einen Verweis auf zusätzliche Information außerhalb der Sicherheitsvorgaben behoben werden und eine oder beide Spezifikationen müssen berichtigt werden.

Formale Sicherheitsmodelle

2.81 Bei den Evaluationsstufen ab E4 muß dem EVG ein Modell einer Sicherheitspolitik (Sicherheitsmodell) zugrunde liegen, d.h. es muß eine abstrakte Beschreibung der wichtigen Sicherheitsprinzipien vorhanden sein, denen der EVG genügt. Es muß in einer formalen Darstellungsform vorliegen, als ein **formales Sicherheitsmodell**. Auf ein geeignetes veröffentlichtes Modell kann ganz oder teilweise Bezug genommen werden oder es muß ein Modell als Teil der Sicherheitsvorgaben vorhanden sein. Jede der oben beschriebenen Darstellungsformen einer formalen Spezifikation kann benutzt werden, um solch ein Modell zu definieren.

2.82 Das formale Modell muß nicht alle sicherheitsspezifischen Funktionen enthalten, die in den Sicherheitsvorgaben angegeben sind. Jedoch muß eine informelle Interpretation des Modells mit Bezug auf die Aussagen in den Sicherheitsvorgaben vorhanden sein. Es muß gezeigt werden, daß die Sicherheitsvorgaben die zugrunde liegende Sicherheitspolitik umsetzen und keine Funktionen enthalten, die mit der zugrunde liegenden Politik im Widerspruch stehen.

2.83 Beispiele für veröffentlichte formale Sicherheitsmodelle sind:

a) Das Bell-La-Padula-Modell [BLP] - ein Modell für Anforderungen an die Zugriffskontrolle, die für eine nationale Sicherheitspolitik zur Vertraulichkeit von Daten typisch sind.

b) Das Clark und Wilson Modell [CWM] - ein Modell für Integritätsanforderungen an kommerzielle Transaktionssysteme.

c) Das Brewer-Nash-Modell [BNM] - ein Modell für Anforderungen an die Zugriffskontrolle im Hinblick auf Kundenvertraulichkeit; typisch für Finanzinstitutionen.

d) Das Eizenberg-Modell [EZBM] - ein Modell für Zugriffsrechte, die sich mit der Zeit ändern.

e) Das Landwehr-Modell [LWM] - ein Modell für Anforderungen an die Datenübertragung eines Nachrichtenverarbeitungsnetzes.

3 VERTRAUENSWÜRDIGKEIT - WIRKSAMKEIT

Einleitung

3.1 Das vorliegende Kapitel erläutert die Evaluationskriterien unter dem Wirksamkeitsaspekt der Vertrauenswürdigkeit eines Evaluationsgegenstandes (EVG). Grundlage der Evaluation sind die Sicherheitsvorgaben, die in Kapitel 2 beschrieben sind. Anhand der Sicherheitsvorgaben wird der EVG gleichzeitig sowohl gemäß den Kriterien dieses Kapitels bezüglich der Wirksamkeit als auch gemäß den im folgenden Kapitel 4 beschriebenen Kriterien bezüglich der Korrektheit evaluiert.

Beschreibung des Ansatzes

3.2 Die Bewertung der Wirksamkeit erfordert die Betrachtung der folgenden Aspekte des EVG:

a) die Eignung der sicherheitsspezifischen Funktionen des EVG, den in den Sicherheitsvorgaben aufgezählten Bedrohungen zu widerstehen;

b) die Fähigkeit der sicherheitsspezifischen Funktionen und Mechanismen des EVG, in einer Weise zusammenzuwirken, daß sie sich gegenseitig unterstützen und ein integriertes, wirksames Ganzes bilden;

c) die Fähigkeit der Sicherheitsmechanismen des EVG, einem direkten Angriff zu widerstehen;

d) ob bekannte Sicherheitsschwachstellen in der *Konstruktion* des EVG in der Praxis die Sicherheit des EVG kompromittieren können;

e) daß der EVG nicht in einer Weise konfiguriert werden kann, die unsicher ist, aber von der ein **Systemverwalter** oder ein Endnutzer vernünftigerweise glauben könnte, daß sie sicher ist;

f) ob bekannte Sicherheitsschwachstellen beim *Betrieb* des EVG in der Praxis die Sicherheit des EVG kompromittieren können.

3.3 Die Bewertung der einzelnen oben beschriebenen Aspekte der Wirksamkeit wird durchgeführt unter Verwendung der Dokumentation, die der Auftraggeber zur Verfügung stellt, und von Dokumentation und Ergebnissen aus der Evaluation der Korrektheit des EVG. Obwohl die Evaluation der Wirksamkeit parallel zur Evaluation der Korrektheit erfolgen kann, kann sie deshalb nicht abgeschlossen werden, bevor die abschließenden Ergebnisse der Bewertung der Korrektheit zur Verfügung stehen.

3.4 Die Untersuchung der Wirksamkeit basiert auf einer Schwachstellenanalyse des EVG. Bei dieser Analyse werden alle Wege gesucht, die es einem Benutzer des EVG erlauben würden, die sicherheitsspezifischen Funktionen und Mechanismen zu deaktivieren, zu umgehen, zu verändern, auszuschalten, direkt anzugreifen oder anderweitig außer Kraft zu setzen. Die Schwachstellenanalyse des Antragstellers muß zumindest alle Informationen in Betracht ziehen, die für die angestrebte Evaluationsstufe in Abbildung 4 angegeben sind (d.h. die Suche nach Schwachstellen wird durchgeführt unter Verwendung der für die Evaluationsstufe insgesamt zur Verfügung gestellten Information). Mit ansteigenden Evaluationsstufen verlangen die Korrektheitskriterien des Kapitels 4, daß die Information, die in Abbildung 4 aufgeführt ist, mit zunehmender Genauigkeit vorgelegt wird, was durch die Verwendung der Verben *darlegen*, *beschreiben* und *erklären* ausgedrückt wird.

3.5 Alle kritischen Sicherheitsmechanismen (d.h. diejenigen, deren Versagen eine Sicherheitslücke hervorrufen würde), werden hinsichtlich ihrer Fähigkeit bewertet, einem direkten Angriff zu widerstehen. Die Mindeststärke jedes **kritischen Mechanismus** wird entweder als *niedrig*, *mittel* oder *hoch* bewertet.

3.6 Damit die Mindeststärke eines kritischen Mechanismus als niedrig eingestuft werden kann, muß erkennbar sein, daß er Schutz gegen zufälliges unbeabsichtigtes Eindringen bietet, während er durch sachkundige Angreifer überwunden werden kann.

3.7 Damit die Mindeststärke eines kritischen Mechanismus als mittel eingestuft werden kann, muß erkennbar sein, daß er Schutz gegen Angreifer mit beschränkten Gelegenheiten oder Betriebsmitteln bietet.

3.8 Damit die Mindeststärke eines kritischen Mechanismus als hoch eingestuft werden kann, muß erkennbar sein, daß er nur von Angreifern überwunden werden kann, die über sehr gute Fachkenntnisse, Gelegenheiten und Betriebsmittel verfügen, wobei ein solcher erfolgreicher Angriff als normalerweise nicht durchführbar beurteilt wird.

3.9 Ein EVG wird eine Evaluation aus Gründen der Wirksamkeit nur dann nicht bestehen, wenn während der Evaluation der Wirksamkeit eine auswertbare Schwachstelle gefunden wurde, die nicht vor Ende der Evaluation behoben wurde. Dies schließt Methoden für einen erfolgreichen direkten Angriff ein, die während der Bewertung der Mindeststärke der Mechanismen gefunden wurden und welche die angegebene Mindeststärke ungültig machen. Wenn irgendeine solche Schwachstelle vorhanden ist, wird der EVG eine Bewertung von E0 erhalten, was bedeutet, daß er für den vorgeschlagenen Einsatz nicht geeignet ist.

3.10 Die Wirksamkeit eines EVG wird immer vor dem Hintergrund der vorhandenen Sicherheitsvorgaben bewertet. Z.B. kann ein Sicherheitsprodukt, das für den Einbau in Systeme verkauft wird, bekannte **verdeckte Kanäle** enthalten. Wenn die Sicherheitsvorgaben jedoch keine Anforderungen an Zugriffskontrolle in Bezug auf Vertraulichkeit enthalten, ist das Vorhandensein von verdeckten Kanälen in dem Produkt ohne Bedeutung. Es wird sich nicht auf die Möglichkeit des EVG auswirken, seine Sicherheitsvorgaben zu erfüllen und wird nicht dazu führen, daß der EVG die Evaluation nicht besteht. Sind Anforderungen an die Zugriffskontrolle in Bezug auf Vertraulichkeit

vorhanden, so können die Sicherheitsvorgaben eine akzeptierbare maximale Bandbreite für die verdeckten Kanäle vorgeben. Wenn gefundene verdeckte Kanäle diese Bandbreite überschreiten oder falls keine Bandbreite vorgegeben wurde, so muß der Evaluator entscheiden, ob die festgestellten verdeckten Kanäle dazu führen, daß der EVG die Evaluation wegen ungeeigneter Funktionalität nicht besteht.

Systeme und Produkte

3.11 Es gibt unterschiedliche Anforderungen und Optionen bezüglich des Inhalts der Sicherheitsvorgaben für einen EVG; diese hängen davon ab, ob es sich bei dem EVG um ein System oder ein Produkt handelt. Diese Unterschiede werden unter Konstruktion - Phase 1 - Forderungen in Kapitel 4 dargestellt und in Kapitel 2 weiter erklärt.

Wirksamkeitskriterien - Konstruktion

Dokumentation

3.12 Der Antragsteller muß, zusätzlich zu der für die Evaluation der Korrektheit erforderlichen Dokumentation, folgende Unterlagen zur Verfügung stellen:

- Analyse der Eignung
- Analyse des Zusammenwirkens
- Analyse der Stärke der Mechanismen
- Liste der bekannten Schwachstellen in der Konstruktion.

Aspekt 1 - Eignung der Funktionalität

Definition

3.13 Als Teil der für die Evaluation der Korrektheit geforderten Dokumentation stellt der Antragsteller die Sicherheitsvorgaben zur Verfügung. Im Verlauf der Korrektheitsbewertung werden diese auf Vollständigkeit und Konsistenz geprüft. Für den Aspekt der Wirksamkeit werden die Sicherheitsvorgaben als Grundlage verwendet um festzustellen, ob die sicherheitsspezifischen Funktionen und Mechanismen des EVG den in den Sicherheitsvorgaben identifizierten Bedrohungen der Sicherheit des EVG auch tatsächlich entgegenwirken.

Anforderungen an Inhalt und Form

3.14 Die Analyse der Eignung muß die sicherheitsspezifischen Funktionen und Mechanismen den in den Sicherheitsvorgaben identifizierten Bedrohungen zuordnen, denen sie entgegenwirken müssen.

Anforderungen an Nachweise

3.15 Die Analyse der Eignung muß zeigen, wie die sicherheitsspezifischen Funktionen und Mechanismen den identifizierten Bedrohungen entgegenwirken. Sie muß zeigen, daß es keine identifizierten Bedrohungen gibt, denen nicht eine oder mehrere der aufgeführten sicherheitsspezifischen Funktionen angemessen entgegenwirken. Diese Analyse muß unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 für die angestrebte Evaluationsstufe angegeben sind.

Aufgaben des Evaluators

3.16 Es ist zu überprüfen, ob die Analyse der Eignung alle Anforderungen hinsichtlich Inhalt, Form und Nachweis erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 für die angestrebte Evaluationsstufe angegeben sind.

Aspekt 2 - Zusammenwirken der Funktionalität

Definition

3.17 Dieser Aspekt der Wirksamkeit untersucht die Fähigkeit der sicherheitsspezifischen Funktionen und Mechanismen des EVG so zusammenzuwirken, daß sie sich gegenseitig unterstützen und ein integriertes, wirksames Ganzes bilden.

Anforderungen an Inhalt und Form

3.18 Die Analyse des Zusammenwirkens muß eine Analyse aller möglichen Beziehungen zwischen den sicherheitsspezifischen Funktionen und Mechanismen zur Verfügung stellen.

Anforderungen an Nachweise

3.19 Die Analyse des Zusammenwirkens muß zeigen, daß es nicht möglich ist, eine sicherheitsspezifische Funktion oder einen Mechanismus dazu zu veranlassen, mit den Aufgaben anderer sicherheitsspezifischer Funktionen oder Mechanismen in Konflikt zu geraten oder ihnen entgegenzuwirken. Diese Analyse muß unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 für die angestrebte Evaluationsstufe angegeben sind.

Aufgaben des Evaluators

3.20 Es ist zu überprüfen, ob die Analyse des Zusammenwirkens alle Anforderungen hinsichtlich Inhalt, Form und Nachweis erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 für die angestrebte Evaluationsstufe angegeben sind.

Aspekt 3 - Stärke der Mechanismen

Definition

3.21 Selbst wenn ein sicherheitsspezifischer Mechanismus nicht umgangen, außer Kraft gesetzt oder anders korrumpiert werden kann, kann es trotzdem möglich sein, ihn durch einen direkten Angriff zu überwinden, der auf Mängel in seinen zugrundeliegenden Algorithmen, Prinzipien oder Eigenschaften zurückzuführen ist. Für diesen Aspekt der Wirksamkeit wird die Fähigkeit der Mechanismen bewertet, solchen direkten Angriffen zu widerstehen. Dieser Aspekt der Wirksamkeit unterscheidet sich von anderen Aspekten darin, daß er den Aufwand an Betriebsmitteln betrachtet, die ein Angreifer benötigen würde, um einen erfolgreichen direkten Angriff durchzuführen.

Anforderungen an Inhalt und Form

3.22 Die Analyse der Stärke der Mechanismen muß alle sicherheitsspezifischen Mechanismen auflisten, die innerhalb des EVG als kritisch festgestellt wurden. Sie muß Analysen über die Algorithmen, Prinzipien und Eigenschaften enthalten, die diesen Mechanismen zugrundeliegen oder sie muß auf solche Analysen verweisen.

Forderungen an Nachweise

3.23 Die Analyse der Stärke der Mechanismen muß aufzeigen, daß alle kritischen Mechanismen die Definition der beanspruchten Einstufung der Mindeststärke, wie in den Paragraphen 3.6 bis 3.8 beschrieben, erfüllen: im Fall von kryptographischen Mechanismen muß dies durch eine Aussage der zuständigen nationalen Behörde erfolgen. Andere Analysen müssen unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 für die angestrebte Evaluationsstufe angegeben sind.

Aufgaben des Evaluators

3.24 Es ist zu überprüfen, ob alle Mechanismen, die kritisch sind, als solche identifiziert wurden. Es ist zu überprüfen, ob die vorgelegte Analyse der Stärke der Mechanismen alle Anforderungen bezüglich Inhalt, Form und Nachweis erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 für die angestrebte Evaluationsstufe angegeben sind. Es ist zu überprüfen, ob die Spezifikationen/Definitionen aller kritischen Mechanismen die beanspruchte Mindeststärke

gewährleisten. Wo erforderlich, sind **Penetrationstests** durchzuführen, um die Mindeststärke der Mechanismen zu bestätigen oder zu verwerfen.

Aspekt 4 - Bewertung der Konstruktionsschwachstellen

Definition

3.25 Vor und während der Betrachtung der anderen Aspekte bei der Evaluation eines EVG werden sowohl durch den Antragsteller als auch durch den Evaluator verschiedene Schwachstellen (z.B. Wege um die sicherheitsspezifischen Funktionen und Mechanismen zu deaktivieren, zu umgehen, zu verändern, auszuschalten) in der Konstruktion des EVG festgestellt worden sein. Für diesen Aspekt der Wirksamkeit werden die so erkannten Schwachstellen bewertet, um herauszufinden, ob durch sie in der Praxis die Sicherheit des EVG, wie sie in den Sicherheitsvorgaben spezifiziert ist, kompromittiert werden kann.

Anforderungen an Inhalt und Form

3.26 Die Liste der Schwachstellen, die durch den Antragsteller vorgelegt werden muß, muß alle ihm bekannten Schwachstellen in der Konstruktion des EVG aufführen. Sie muß jede Schwachstelle ansprechen, eine Analyse ihrer möglichen Auswirkungen be-inhalten und die Maßnahmen aufzeigen, die zur Abhilfe vorgeschlagen oder zur Verfügung gestellt werden.

Anforderungen an Nachweise

3.27 Die Analyse der möglichen Auswirkungen jeder bekannten Schwachstelle muß aufzeigen, daß die betreffende Schwachstelle in der beabsichtigten Einsatzumgebung des EVG nicht ausgenutzt werden kann, weil entweder

- die Schwachstelle angemessen durch andere, nicht beeinträchtigte Sicherheitsmechanismen geschützt ist oder
- gezeigt werden kann, daß die Schwachstelle in Bezug zu den Sicherheitsvorgaben ohne Bedeutung ist, in der Praxis nicht existieren wird oder daß ihr angemessen durch dokumentierte technische, personelle, organisatorische oder materielle Sicherheitsmaßnahmen außerhalb des EVG entgegengewirkt werden kann. Diese externen Sicherheitsmaßnahmen müssen in der entsprechenden Dokumentation beschrieben (oder hinzugefügt worden) sein.

Die Analyse muß unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 für die angestrebte Evaluationsstufe angegeben sind.

Aufgaben des Evaluators

3.28 Es ist zu überprüfen, ob die Liste der bekannten Schwachstellen in der Konstruktion alle Forderungen bezüglich Inhalt, Form und Nachweis, so wie oben beschrieben, erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 für die angestrebte Evaluationsstufe angegeben sind. Es ist eine eigene Schwachstellenanalyse unter Berücksichtigung der aufgelisteten und der während der Evaluation gefundenen Schwachstellen durchzuführen. Es ist zu überprüfen, ob alle Kombinationen von bekannten Schwachstellen untersucht wurden. Es ist zu überprüfen, ob die Analysen der möglichen Auswirkungen der Schwachstellen keine undokumentierten oder unvernünftigen Annahmen über die vorgesehene Einsatzumgebung enthalten. Es ist zu überprüfen, ob alle Annahmen und Anforderungen bezüglich externer Sicherheitsmaßnahmen ausreichend dokumentiert wurden. Es sind Penetrationstests durchzuführen, um zu bestätigen oder zu widerlegen, ob die bekannten Schwachstellen in der Praxis wirklich ausgenutzt werden können.

Wirksamkeitskriterien - Betrieb

Dokumentation

3.29 Der Antragsteller muß zusätzlich zu der für die Korrektheits-Evaluation erforderlichen Dokumentation folgende Unterlagen zur Verfügung stellen:

- Analyse der Benutzerfreundlichkeit
- Liste der bekannten Schwachstellen bei der operationellen Nutzung

Aspekt 1 - Benutzerfreundlichkeit

Definition

3.30 Dieser Aspekt der Wirksamkeit untersucht, ob ein EVG in einer Weise konfiguriert oder benutzt werden kann, die unsicher ist, aber bei der ein Administrator oder ein Endnutzer des EVG vernünftigerweise davon ausgeht, daß er sicher ist.

Anforderungen an Inhalt und Form

3.31 Die Analyse der Benutzerfreundlichkeit muß mögliche Betriebsarten des EVG beschreiben, einschließlich des Betriebes nach Bedien- oder Betriebsfehlern, und ihre Konsequenzen und Folgerungen für die Aufrechterhaltung eines sicheren Betriebes.

Anforderungen an Nachweise

3.32 Die Analyse der Benutzerfreundlichkeit muß aufzeigen, daß jeder menschliche oder andere Fehler, der sicherheitsspezifischen Funktionen oder Mechanismen ausschaltet oder unbrauchbar macht, leicht festzustellen ist. Sie muß zeigen, daß es erkennbar ist, wenn ein EVG in einer Weise konfiguriert oder benutzt werden kann, die unsicher ist (d.h. die sicherheitsspezifischen Funktionen und Mechanismen des EVG erfüllen die Sicherheitsvorgaben nicht), obwohl ein Endnutzer oder Administrator vernünftigerweise von einem sicheren Zustand ausgehen kann. Die Analyse muß unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 für die angestrebte Evaluationsstufe angegeben sind.

Aufgaben des Evaluators

3.33 Es ist zu überprüfen, ob die vorgelegte Analyse der Benutzerfreundlichkeit alle Anforderungen hinsichtlich Inhalt, Form und Nachweis erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 für die angestrebte Evaluationsstufe angegeben sind. Die Analyse ist nach undokumentierten oder unvernünftigen Annahmen über die vorgesehene Betriebsumgebung zu überprüfen. Es ist zu überprüfen, ob alle Annahmen und Forderungen zu externen Sicherheitsmaßnahmen (wie z.B. externe prozedurale, materielle und personelle Kontrollmaßnahmen) ordnungsgemäß dokumentiert wurden. Jede Konfigurations- und Installationsprozedur ist nachzuvollziehen, um zu überprüfen, ob der EVG sicher konfiguriert und benutzt werden kann. Dabei ist lediglich die Dokumentation für den Nutzer und für den Administrator als Grundlage zu benutzen. Wo erforderlich, sind zusätzliche Tests durchzuführen, um die Analyse der Benutzerfreundlichkeit zu bestätigen oder zu widerlegen.

Aspekt 2 - Bewertung der operationellen Schwachstellen

Definition

3.34 Vor und während der Betrachtung der anderen Aspekte bei der Evaluation eines EVG werden sowohl durch den Antragsteller als auch durch den Evaluator verschiedene operationelle Schwachstellen des EVG festgestellt worden sein. Für diesen Aspekt der Wirksamkeit werden die so erkannten Schwachstellen bewertet, um herauszufinden, ob durch sie in der Praxis die Sicherheit des EVG, wie sie in den Sicherheitsvorgaben spezifiziert ist, kompromittiert werden kann.

Anforderungen an Inhalt und Form

3.35 Die Liste der Schwachstellen, die durch den Auftraggeber vorgelegt werden muß, muß alle ihm bekannten operationellen Schwachstellen des EVG aufführen. Sie muß jede Schwachstelle ansprechen, eine Analyse ihrer möglichen Auswirkungen beinhalten und

die Maßnahmen aufzeigen, die zur Abhilfe vorgeschlagen oder zur Verfügung gestellt werden.

Anforderungen an Nachweise

3.36 Die Analyse der möglichen Auswirkungen jeder bekannten Schwachstelle muß aufzeigen, daß die betreffende Schwachstelle in der beabsichtigten Einsatzumgebung des EVG nicht ausgenutzt werden kann, weil entweder

- die Schwachstelle angemessen durch andere, nicht beeinträchtigte externe Sicherheitsmaßnahmen geschützt ist oder
- gezeigt werden kann, daß die Schwachstelle bezüglich der Sicherheitsvorgaben ohne Bedeutung ist oder in der Praxis nicht ausgenützt werden kann.

Die Analyse muß unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 für die angestrebte Evaluationsstufe angegeben sind. Alle geforderten externen Sicherheitsmaßnahmen müssen in der entsprechenden Dokumentation beschrieben (oder hinzugefügt worden) sein.

Aufgaben des Evaluators

3.37 Es ist zu überprüfen, ob die Liste der bekannten operationellen Schwachstellen alle Anforderungen bezüglich Inhalt, Form und Nachweis, so wie oben beschrieben, erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 für die angestrebte Evaluationsstufe angegeben sind. Es ist eine eigene Schwachstellenanalyse unter Berücksichtigung der aufgelisteten und der während der Evaluation gefundenen Schwachstellen durchzuführen. Es ist zu überprüfen, ob alle Kombinationen von bekannten Schwachstellen untersucht wurden. Es ist zu überprüfen, ob die Analysen der möglichen Auswirkungen keine undokumentierten oder unvernünftigen Annahmen über die vorgesehene Einsatzumgebung enthalten. Es ist zu überprüfen, ob alle Annahmen und Forderungen zu externen Sicherheitsmaßnahmen ausreichend dokumentiert wurden. Es sind Penetrationstests durchzuführen, um zu bestätigen oder zu widerlegen, ob die bekannten Schwachstellen in der Praxis wirklich ausgenutzt werden können.

Informationen, die bei der Korrektheitsbewertung erarbeitet wurden und die bei der Durchführung der Schwachstellenanalyse zu verwenden sind

INFORMATION	E1	E2	E3	E4	E5	E6
Sicherheitsvorgaben (Bedrohungen, Ziele, Funktionen, Mechanismen, Evaluationsstufe, Mechanismusstärke)	√	√	√	√	√	√
Formals Sicherheitsmodell				√	√	√
Funktionen (informell)	√	√	√	√	√	√
Funktionen (semiformal)				√	√	
Funktionen (formal)						√
Architektur-Entwurf (informell)	√	√	√			
Architektur-Entwurf (semiformal)				√	√	
Architektur-Entwurf (formal)						√
Fein-Entwurf (informell)			√			
Fein-Entwurf (semiformal)				√	√	√
Implementierung (Hardware-zeichnungen und Quellcode)				√	√	√
Implementierung (Objekt-code)						√
Betrieb (User/Systemverwalter-dokumentation, Auslieferung und Konfigurierung, Anlauf und Betrieb	√	√	√	√	√	√
	darlegen		Beschreiben		erklären	
	Stufe der Anforderung					

Abb. 4 Zur Schwachstellenanalyse verwendete Informationen

4 VERTRAUENSWÜRDIGKEIT - KORREKTHEIT

Einleitung

4.1 Das vorliegende Kapitel beschreibt die Evaluationskriterien bezüglich des Korrektheitsaspektes der Vertrauenswürdigkeit eines Evaluationsgegenstandes (EVG). Die Basis für die Evaluation sind die Sicherheitsvorgaben laut Definition in Kapitel 2. Die Sicherheitsvorgaben müssen für ein System oder Produkt alle notwendigen Informationen, wie in Kapitel 2 beschrieben, enthalten. Hierzu gehören auch die angestrebte Evaluationsstufe und die angestrebte Mindeststärke der Mechanismen. Der Wirksamkeitsaspekt der Vertrauenswürdigkeit wird durch die in Kapitel 3 dargelegten Kriterien abgedeckt.

Charakterisierung

4.2 Sieben Evaluationsstufen wurden bezüglich des Vertrauens in die Korrektheit eines EVG definiert. E0 bezeichnet die niedrigste, E6 die höchste dieser Stufen.

4.3 Die sieben Evaluationsstufen können wie folgt *charakterisiert* werden:

Stufe E0

4.4 Diese Stufe repräsentiert unzureichende Vertrauenswürdigkeit.

Stufe E1

4.5 Auf dieser Stufe müssen für den EVG die Sicherheitsvorgaben und eine informelle Beschreibung des Architekturentwurfs vorliegen. Durch funktionale Tests muß nachgewiesen werden, daß der EVG die Anforderungen der Sicherheitsvorgaben erfüllt.

Stufe E2

4.6 Zusätzlich zu den Anforderungen für die Stufe E1 muß hier eine informelle Beschreibung des Feinentwurfs vorliegen. Die Aussagekraft der funktionalen Tests muß bewertet werden. Ein Konfigurationskontrollsystem und ein genehmigtes Distributionsverfahren müssen vorhanden sein.

Stufe E3

4.7 Zusätzlich zu den Anforderungen für die Stufe E2 müssen der Quellcode bzw. die Hardware-Konstruktionszeichnungen, die den Sicherheitsmechanismen entsprechen, bewertet werden. Die Aussagekraft der Tests dieser Mechanismen muß bewertet werden.

Stufe E4

4.8 Zusätzlich zu den Anforderungen für die Stufe E3 muß ein formales Sicherheitsmodell Teil der Sicherheitsvorgaben sein. Die sicherheitsspezifischen Funktionen, der Architekturentwurf und der Feinentwurf müssen in semiformaler Notation vorliegen.

Stufe E5

4.9 Zusätzlich zu den Anforderungen für die Stufe E4 muß ein enger Zusammenhang zwischen dem Feinentwurf und dem Quellcode bzw. den Hardware-Konstruktionszeichnungen bestehen.

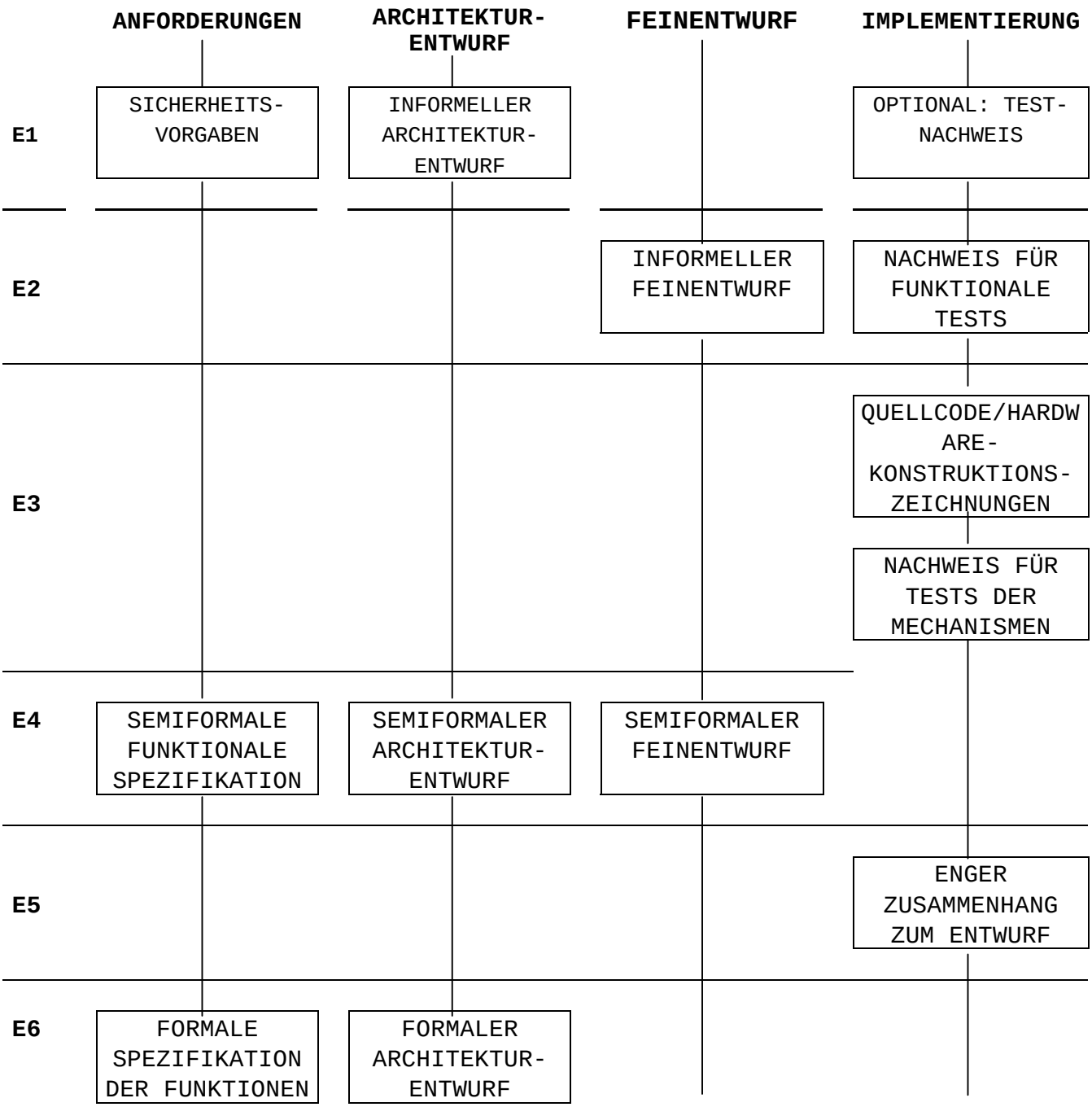
Stufe E6

4.10 Zusätzlich zu den Anforderungen für die Stufe E5 müssen die sicherheitsspezifischen Funktionen und der Architekturentwurf in einer formalen Notation vorliegen, die konsistent mit dem zugrundeliegenden formalen Sicherheitsmodell ist.

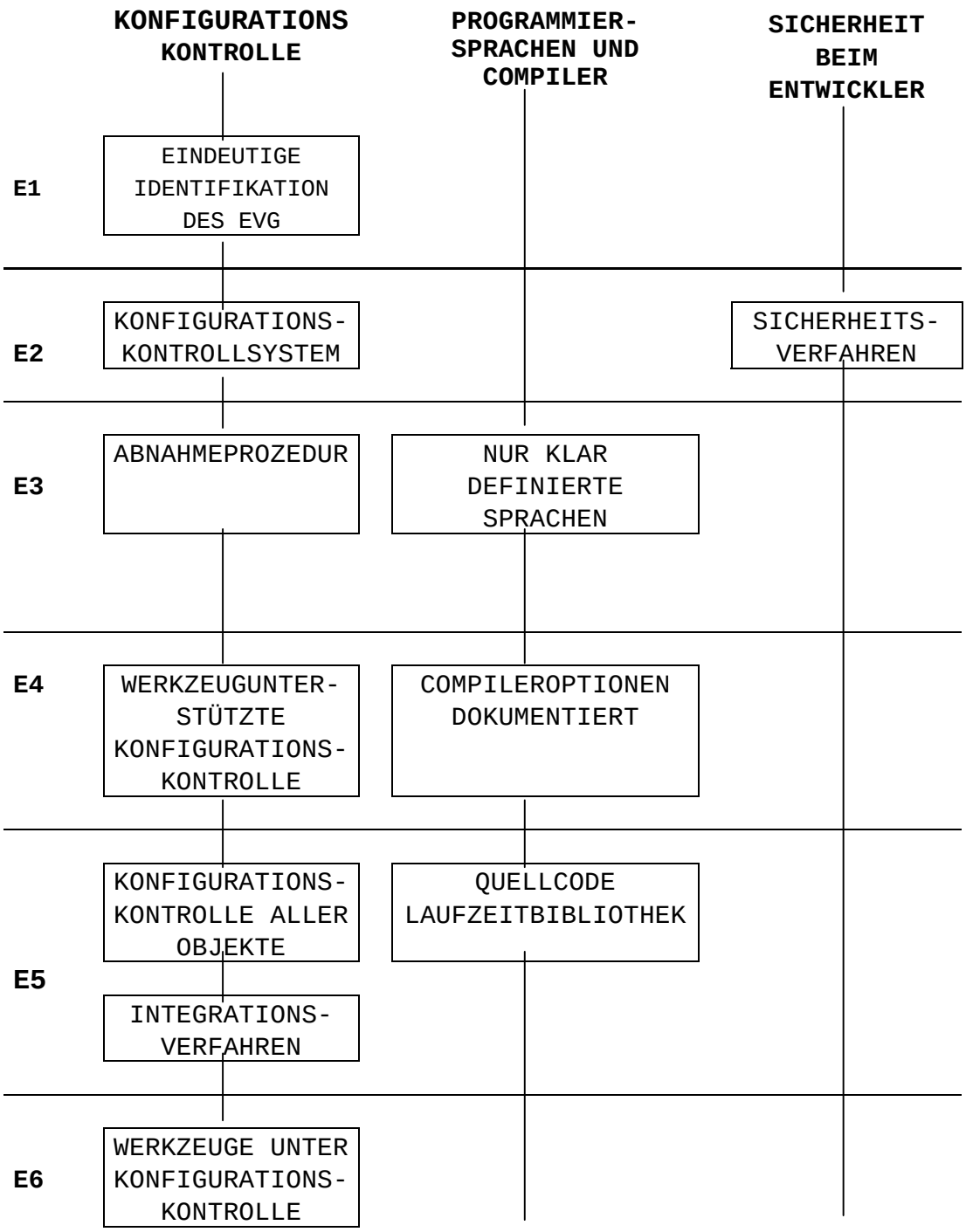
Zusammenfassung der Forderungen

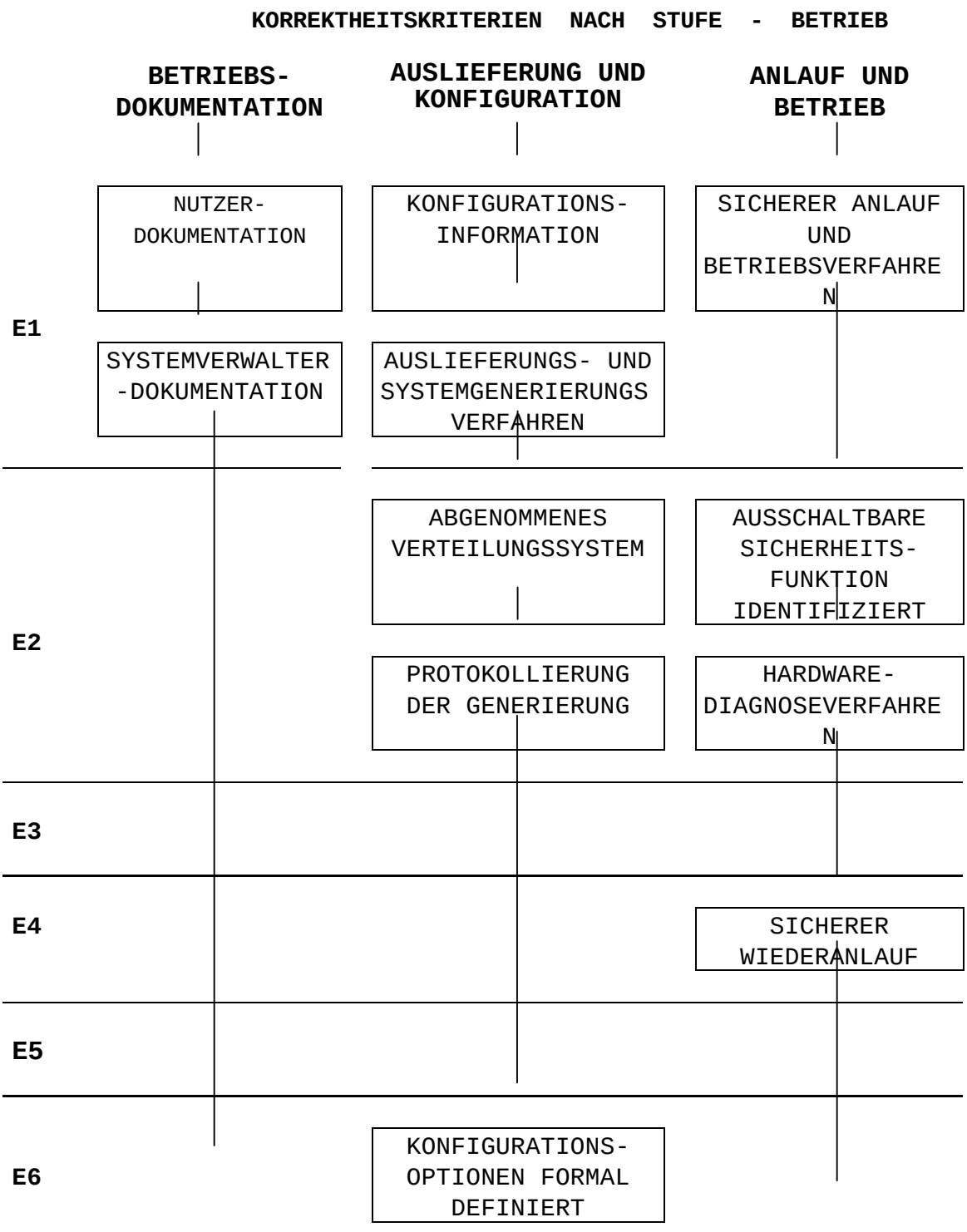
4.11 Die weiteren Abschnitte des Kapitels enthalten die detaillierten Kriterien, die für jede Evaluationsstufe bezüglich der Korrektheit erfüllt werden müssen, unter Einzelüberschriften, die für jede der Stufen von E1 bis E6 wiederholt werden. Die Hauptunterschiede zwischen den Stufen ergeben sich aus zusätzlichen Anforderungen an die Überprüfung des Entwicklungsprozesses. Zum besseren Verständnis dieser Unterschiede zeigt das folgende Diagramm die Beziehung zwischen den vom Antragsteller zu liefernden Hauptobjekten und der Evaluationsstufe, auf welcher sie zuerst vom Evaluator verlangt werden.

KORREKTHEITSKRITERIEN NACH STUFE - ENTWICKLUNGSPROZESS



KORREKTHEITSKRITERIEN NACH STUFE - ENTWICKLUNGSUMGEBUNG




KORREKTHEITSKRITERIEN NACH STUFE - BETRIEB
BETRIEBS-DOKUMENTATION
AUSLIEFERUNG UND KONFIGURATION
ANLAUF UND BETRIEB
NUTZER-DOKUMENTATION
KONFIGURATIONS-INFORMATION
SICHERER ANLAUF UND BETRIEBSVERFAHREN
E1
SYSTEMVERWALTER-DOKUMENTATION
AUSLIEFERUNGS- UND SYSTEMGENERIERUNGS VERFAHREN
ABGENOMMENES VERTEILUNGSSYSTEM
AUSSCHALTBARE SICHERHEITS-FUNKTION IDENTIFIZIERT
E2
PROTOKOLLIERUNG DER GENERIERUNG
HARDWARE-DIAGNOSEVERFAHREN
E3
E4
SICHERER WIEDERANLAUF
E5
E6
KONFIGURATIONS-OPTIONEN FORMAL DEFINIERT

Beschreibungsansatz

4.12 Die Evaluationskriterien für die Bewertung der Korrektheit unterscheiden zwischen Kriterien bezüglich der Art und Weise, in welcher der EVG entwickelt wird (Konstruktion), und Kriterien zur Art und Weise seiner künftigen Verwendung (Betrieb). Für jede einzelne Evaluationsstufe werden diese Evaluationskriterien unter verschiedenen Phasen und Aspekten weiter aufgegliedert.

4.13 Für jeden Aspekt bzw. jede Phase wird die zur Prüfung bereitzustellende Dokumentation angegeben; es folgen Anforderungen an deren Inhalt und Form oder an die Verfahren und Standards, die sie zu definieren hat; hieran schließen sich die jeweiligen Nachweise an, anhand derer die Erfüllung der betreffenden Kriterien zu zeigen ist, und zum Schluß werden die Aufgaben angegeben, die durch den Evaluator durchgeführt werden müssen.

4.14 Da auf den einzelnen Evaluationsstufen deutlich unterschiedliche Anforderungen gestellt werden, sind die Kriterien aus Gründen der Klarheit für jede Stufe separat dargestellt. Neue oder geänderte Anforderungen auf den einzelnen Stufen sind **fett** gedruckt. Auf den höheren Stufen besteht ein allgemeines Bedürfnis nach größerer Strenge und Tiefe der Nachweise. Dieser Sachverhalt spiegelt sich wider durch den Gebrauch der Verben "*darlegen*" (state), "*beschreiben*" (describe) und "*erklären*" (explain) auf den verschiedenen Stufen im Zusammenhang mit vielen Kriterien bezüglich des Inhalts und der Form, die sich ansonsten nicht ändern.

4.15 Abgesehen von der Stufe E1 liegt die Aufgabe der Bereitstellung von Nachweisen beim Antragsteller. Diese werden dann vom Evaluator überprüft oder bestätigt. Der Evaluator hat zusätzliche Nachweise nur dann zu erbringen, wenn Maßnahmen von dritter Seite erforderlich werden, um das benötigte Vertrauen zu schaffen. Es gibt z.B. Anforderungen an den Antragsteller und den Evaluator, Nachweise für dynamisches Testen zu liefern. Die Hauptaufgabe des Antragstellers besteht darin, Nachweise, insbesondere Testpläne und Testergebnisse vorzulegen, die als Teil seines normalen Entwicklungsverfahrens für das betreffende System oder Produkt erzeugt werden. Aufgabe des Evaluators ist es, nachzuweisen, daß er die vom Antragsteller bereitgestellten Ergebnisse überprüft und daß er daneben auch eigene Tests durchgeführt hat, um die Vollständigkeit, Spannweite und Genauigkeit der Tests des Antragstellers zu überprüfen. Ebenso muß er offensichtliche Inkonsistenzen oder Fehler, die in den Ergebnissen der Tests des Antragstellers gefunden wurden, ansprechen.

4.16 Testen ist nur ein Aspekt der Qualitätssicherung. Durch die Kriterien hinweg wird angenommen, daß ein Qualitätssicherungsprogramm eingeführt wurde, das über den gesamten Lebenszyklus des Evaluationsgegenstandes Anwendung findet. Dieses Qualitätssicherungsprogramm hat die Erzeugung, Instandhaltung und Vernichtung aller Dokumente, Programme und Hardware im Bezug zum EVG zu umfassen. Die niedergeschriebenen Kriterien können Qualitätssicherern helfen zu erkennen, ob ihr Qualitätssicherungsprogramm für die angestrebte Evaluationsstufe des EVG ausreichend ist.

Darstellung der Kriterien für die Korrektheit

4.17 Die folgenden Abschnitte beschreiben den Aufbau und Inhalt der Kriterien, der für jede der Evaluationsstufen E1 bis E6 verwendet wird. Sie sind für jede Stufe gültig und werden nicht für jede wiederholt. Die einzelnen Paragraphen innerhalb jeder Evaluationsstufe sind wie folgt numeriert:

<Stufen-Bezeichnung>.<Paragraphennummer innerhalb der Stufe>

Damit ist z.B. der dritte Paragraph von E2 auf E2.3 numeriert. Leere Paragraphen sind, wo notwendig, in jeder Stufe eingefügt, so daß gleichnumerierte Paragraphen innerhalb jeder Stufe auf den gleichen Sachverhalt verweisen.

Konstruktion - Der Entwicklungsprozeß

4.18 Eine wichtige Quelle des Vertrauens in die Korrektheit der Sicherheitsaspekte eines EVG ist das Verständnis der Art und Weise, in welcher er entwickelt wurde. Innerhalb dieser Kriterien werden 4 Phasen im Entwicklungsprozeß unterschieden. Faktoren, die zur Ausbildung von Vertrauen beitragen, werden jeweils in den Kriterien für die einzelnen Phasen dieses Prozesses aufgeführt. Unabhängig davon wie ein EVG wirklich entwickelt wurde, muß die zum Nachweis dienende Information den Phasen entsprechen.

Phase 1 - Anforderungen

4.19 Diese erste Phase des Entwicklungsprozesses bezieht sich auf die Erstellung der Sicherheitsvorgaben für das System oder Produkt. Die Sicherheitsvorgaben sind die Basis für die Evaluation. Sie enthalten u.a. die angestrebte Evaluationsstufe und die angestrebte Mindeststärke der Mechanismen.

Phase 2 - Architekturentwurf

4.20 Diese Phase des Entwicklungsprozesses bezieht sich auf die oberste Stufe der Definition und des Entwurfs des EVG. Dies erfolgt in Form einer Spezifikation auf einem hohen Abstraktionsniveau, die die grundlegende Struktur des EVG, seine externen Schnittstellen sowie seine Untergliederung in die wichtigsten Hardware- und Software-Komponenten identifiziert. Die Spezifikation unterscheidet zwischen dem, was der EVG letztendlich tun wird (die "Top-Level-Beschreibung") und wie er dies tun wird (der "Top-Level-Entwurf"). Es ist besonders wichtig, daß im Architekturentwurf Wert auf eine klare und wirksame Trennung zwischen Sicherheitskomponenten und anderen Komponenten gelegt wird. Die Trennung kann physisch erfolgen oder durch in Hard- oder Firmware vorliegende unterstützende Schutzmechanismen oder durch sonstige Maßnahmen erreicht werden. Ein guter Entwurf ermöglicht die Konzentration der Evaluation auf begrenzte Bereiche des EVG, die zur Sicherheit beitragen, und erlaubt der Erfüllung der Sicherheitsvorgaben in dem Maße leicht zu folgen, in welchem der Entwurf nach und nach verfeinert wird.

Phase 3 - Feinentwurf

4.21 Diese Phase des Entwicklungsprozesses bezieht sich auf die Verfeinerung des Architekturentwurfs des EVG bis hin zu einem Detaillierungsgrad, der als Basis für die Programmierung und/oder Hardware-Konstruktion verwendet werden kann, d.h. alle Entwurfs- und Spezifikationsstadien unterhalb des "Architekturentwurfs". Komponenten, die auf der untersten Spezifikationsstufe identifiziert werden, tragen die Bezeichnung Basiskomponenten; aus den Spezifikationen eben dieser Basiskomponenten wird der tatsächliche Code und/oder die Hardware erstellt. Auf dieser Stufe werden die sicherheitsspezifischen Komponenten identifiziert. Ebenfalls auf dieser Stufe werden Komponenten identifiziert, die nicht unmittelbar zur Sicherheit beitragen, deren Fehlverhalten oder Mißbrauch jedoch die Sicherheit gefährden kann. Diese Komponenten sind sicherheitsrelevant, da es von ihrer korrekten Arbeitsweise abhängt, ob der EVG die Sicherheit garantieren kann. Zwischenstufen innerhalb des Feinentwurfs können je nach angewandter Entwicklungsmethode und der Komplexität des EVG existieren. Werden die Spezifikationen des EVG nach und nach detaillierter und weniger abstrakt, so ist es wichtig, daß der Übergang in einer Weise erfolgt, der die Intention des Architekturentwurfs beibehält.

Phase 4 - Implementierung

4.22 Diese Phase des Entwicklungsprozesses bezieht sich auf die Implementierung des Feinentwurfs des EVG als Hardware und/oder Software. Jede Basiskomponente ist zunächst aus den Spezifikationen der Basiskomponenten zu programmieren oder zu konstruieren. Diese einzelnen Basiskomponenten müssen dann gegen ihre Spezifikationen geprüft und getestet werden. Anschließend werden einzelne Basiskomponenten zusammen in kontrollierter Form integriert, bis der komplette EVG vorliegt. Der komplette EVG muß dann als Ganzes gegen die Sicherheitsvorgaben geprüft und getestet werden. Man muß sich hierbei darüber im klaren sein, daß das Testen einer Basiskomponente oder einer komplexeren Einheit gegen ihre Spezifikationen nur Fehler oder Abweichungen von den Spezifikationen aufzeigen kann, niemals jedoch die Abwesenheit von Fehlern. Aus diesem Grund ist es auf den höheren Evaluationsstufen erforderlich, die Tests durch Analysen zu ergänzen.

Konstruktion - Die Entwicklungsumgebung

4.23 Zur Entwicklungsumgebung zählen die Maßnahmen, Verfahren und Standards, die der Entwickler während der Entwicklung, Produktion und Wartung des EVG einsetzt.

Aspekt 1 - Konfigurationskontrolle

4.24 Zur Konfigurationskontrolle zählen die Kontrollen, die der Entwickler bezüglich seiner Entwicklungs-, Produktions- und Wartungsprozesse durchgeführt hat; beispielsweise, um sicherzustellen, daß jegliche Entwurfsergebnisse oder deren Implementierung in kontrollierter Art und Weise erstellt und geändert werden und daß sie nachweislich den früheren Darstellungen entsprechen, auf denen sie aufbauen. Zur Bewertung der Kon-

figurationskontrolle gehört auch das Verständnis der beim Entwickler praktizierten Qualitätsmanagementverfahren. Nach der Auslieferung der ersten Version des EVG ist es fast unausbleiblich, daß Fehlerkorrekturen oder Änderungen zur Erfüllung geänderter Zielsetzungen die Entwicklung und Herausgabe weiterer Versionen des EVG nach sich ziehen. Aus diesem Grund ist es erforderlich, daß die Konfigurationskontrolle des EVG sowie seiner Dokumentation nach der ersten Freigabe und Auslieferung weitergeführt wird. Die Konfigurationskontrolle ist für den Entwickler wichtig um sicherzustellen, daß der EVG nicht in einer Weise verändert wird, welche die Evaluationsergebnisse ungültig macht.

Aspekt 2 - Programmiersprachen und Compiler

4.25 Dieser Aspekt gilt nur für Basiskomponenten, die in Soft- und Firmware implementiert sind. Er enthält Forderungen an die Programmiersprachen, die Werkzeuge zur Compilierung und an die Laufzeitbibliotheken, die für die Entwicklung des EVG benutzt werden.

Aspekt 3 - Sicherheit beim Entwickler

4.26 Unter die Sicherheit beim Entwickler fallen die materiellen, organisatorischen, technischen und personellen Maßnahmen, die innerhalb der Entwicklungsumgebung ergriffen werden. Hierzu zählt die materielle Sicherheit des/der Entwicklungsorte/s sowie Kontrollen bei der Auswahl und Überprüfung des Entwicklungspersonals. Zielsetzung der Sicherheit beim Entwickler ist es, die Entwicklung vor böswilligen Angriffen zu schützen und die Vertraulichkeit von Informationen in geeigneter Weise sicherzustellen.

Betrieb - Die Betriebsdokumentation

4.27 Die Betriebsdokumentation ist das wichtigste Instrument der Kommunikation zwischen dem Entwickler eines EVG und seinen Kunden. Ihre Verständlichkeit, ihr Umfang und ihre Korrektheit sind deshalb wichtige Faktoren für den sicheren Betrieb des EVG. Sie kann in zwei Klassen unterteilt werden: Informationen für Endbenutzer (Benutzerdokumentation) und Informationen für Systemverwalter (Systemverwalter-Dokumentation).

Aspekt 1 - Benutzerdokumentation

4.28 Bei der Benutzerdokumentation handelt es sich um Informationen über den EVG, die der Entwickler dem Endbenutzer zur Verwendung bereitstellt. Diese Dokumentation soll dem Endbenutzer dabei helfen, die Sicherheitseigenschaften des EVG sowie den Beitrag des Endbenutzers zur Aufrechterhaltung der Sicherheit während des Gebrauchs zu verstehen.

Aspekt 2 - Systemverwalter-Dokumentation

4.29 Bei der Systemverwalter-Dokumentation handelt es sich um Informationen über den EVG, die der Entwickler dem Systemverwalter zur Verwendung bereitstellt. Zu diesen

Informationen können auch solche zählen, die für Endbenutzer weder relevant noch geeignet sind. Diese Dokumentation sollte dem Systemverwalter helfen, den EVG in einer sicheren Art und Weise zu installieren und zu bedienen.

Betrieb - Die Betriebsumgebung

4.30 Die Betriebsumgebung umfaßt die Maßnahmen, Verfahren und Standards im Zusammenhang mit einer sicheren Auslieferung und Installation und einem sicheren Betrieb eines EVG. Bei einem bereits in Betrieb befindlichen System ist es möglich, die tatsächlichen Betriebsverfahren zu bewerten. In anderen Fällen ist es lediglich möglich, vorgeschlagene Verfahren zu evaluieren.

Aspekt 1 - Auslieferung und Konfiguration

4.31 Dieser Abschnitt behandelt die Verfahren zur Wahrung der Sicherheit während des Transports des EVG oder seiner Komponenten zum Benutzer, und zwar sowohl mit Blick auf die Erstauslieferung als auch auf später folgende Modifikationen. Hierunter fallen alle speziellen Verfahren oder Maßnahmen, die erforderlich sind, um den EVG während der Installation zu konfigurieren oder die Authentizität des gelieferten EVG nachzuweisen. Solche Verfahren und Maßnahmen sind die Gewähr dafür, daß der durch den EVG angebotene Sicherheitsschutz nicht während des Transportes bzw. durch Eingriffe in die Sicherheitskomponenten während der Installation und Konfiguration am Aufstellungsort beeinträchtigt wird.

Aspekt 2 - Anlauf und Betrieb

4.32 Dieser Abschnitt behandelt die Verfahren, die der Systemverwalter zum sicheren täglichen Betrieb des EVG benutzt. Hierunter darf nicht nur der Alltagsbetrieb (Belange wie z.B. Systemstart) gerechnet werden, sondern auch andere Routineaktivitäten wie beispielsweise die Erstellung notwendiger Sicherungskopien oder die Wartung oder außergewöhnliche Aktivitäten wie Systemneustart und Wiederherstellung nach einem Systemausfall. Fast alle EVG erfordern Wartung, sei es, um geänderte Zielsetzungen zu erfüllen, sei es, um auf Fehler zu reagieren. Aus diesem Grund haben diese Verfahren Bestimmungen für autorisierte Änderungen, Auswechslungen oder Ergänzungen des EVG zu enthalten.

Stufe E1

Konstruktion - Der Entwicklungsprozeß

E1.1 Der Antragsteller muß den EVG und die folgende Dokumentation bereitstellen:

- **Die Sicherheitsvorgaben für den EVG**
- **informelle Beschreibung der Architektur des EVG**
- **`Testdokumentation (optional)`**
- **`Bibliothek der Testprogramme und -werkzeuge, die für den Test des EVG benutzt wurden (optional)`**

Phase 1 - Anforderungen

Anforderungen an Inhalt und Form

E1.2 **Die Sicherheitsvorgaben müssen die sicherheitsspezifischen Funktionen darlegen, die vom EVG zur Verfügung gestellt werden. Im Falle eines Systems müssen die Sicherheitsvorgaben zusätzlich eine System-Sicherheitspolitik (SSP) enthalten, die die Sicherheitsziele und Bedrohungen des Systems identifiziert. Für ein Produkt müssen die Sicherheitsvorgaben zusätzliche Aussagen enthalten, die die Art des Produkteinsatzes, die vorgesehene Einsatzumgebung und die für diese Einsatzumgebung angenommenen Bedrohungen identifizieren. Die in den Sicherheitsvorgaben aufgeführten sicherheitsspezifischen Funktionen müssen in informeller Notation (siehe Kapitel 2) spezifiziert werden.**

Anforderungen an Nachweise

E1.3 **Im Falle eines Systems müssen die Sicherheitsvorgaben darlegen, auf welche Weise die vorgeschlagene Funktionalität die Sicherheitsziele erfüllt und wie sie den definierten Bedrohungen angemessen entgegenwirkt. Im Fall eines Produktes müssen die Sicherheitsvorgaben darlegen, warum die Funktionalität für diese Art des Einsatzes zweckmäßig ist und wie sie den angenommenen Bedrohungen entgegenwirkt.**

Aufgaben des Evaluators

E1.4 **Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist zu überprüfen, ob es Inkonsistenzen innerhalb der Sicherheitsvorgaben gibt.**

Phase 2 - Architekturentwurf

Anforderungen an Inhalt und Form

E1.5 **Diese Beschreibung muß die grundsätzliche Struktur sowie alle externen Schnittstellen des EVG darlegen. Sie muß die Hard- und Firmware darlegen, die der EVG benötigt, und die Funktionalität der unterstützenden Schutzmechanismen angeben, die in dieser Hard- oder Firmware implementiert sind.**

Anforderungen an Nachweise

E1.6 **Die Beschreibung der Architektur muß darlegen, wie die sicherheitsspezifischen Funktionen der Sicherheitsvorgaben zur Verfügung gestellt werden.**

Aufgaben des Evaluators

E1.7 **Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.**

Phase 3 - Feinentwurf

Anforderungen an Inhalt und Form

E1.8 **Keine Anforderungen.**

Anforderungen an Nachweise

E1.9 **Keine Anforderungen.**

Aufgaben des Evaluators

E1.10 **Keine Aufgaben.**

Phase 4 - Implementierung

Anforderungen an Inhalt und Form

E1.11 **Falls die Testdokumentation zur Verfügung gestellt wird, muß sie Testpläne, Testziele, Testverfahren und Testergebnisse enthalten. Falls eine Bibliothek von Testprogrammen zur Verfügung gestellt wird, muß sie Testprogramme und -werkzeuge enthalten, mit denen alle Tests, die in der Testdokumentation beschrieben sind, wiederholt werden können.**

Anforderungen an Nachweise

E1.12 **Falls die Testdokumentation zur Verfügung gestellt wird, muß sie die Übereinstimmung zwischen den Tests und den sicherheitsspezifischen Funktionen in den Sicherheitsvorgaben darlegen.**

Aufgaben des Evaluators

E1.13 **Es sind für alle in den Sicherheitsvorgaben identifizierten sicherheitsspezifischen Funktionen Tests durchzuführen, mit denen geprüft wird, ob der EVG die Sicherheitsvorgaben erfüllt. Zusätzlich sind Tests zur Fehlersuche durchzuführen. Falls auf angemessene Weise nachgewiesen wird, daß solche Tests bereits durch den oder im Auftrag des Antragsteller(s) durchgeführt wurden, ist eine Wiederholung der Tests durch den Evaluator nicht erforderlich. Die Testergebnisse müssen aber von ihm stichprobenhaft überprüft werden.**

Konstruktion - Die Entwicklungsumgebung

E1.14 Der Antragsteller muß die folgende Dokumentation bereitstellen:

- **Konfigurationsliste, die die Version des EVG für die Evaluation identifiziert**

Aspekt 1 - Konfigurationskontrolle

Anforderungen an Inhalt und Form

E1.15 **Die Konfigurationsliste muß darlegen, wodurch der EVG eindeutig identifiziert ist (Versionsnummer).**

Anforderungen an Nachweise

E1.16 **Die Konfigurationsliste muß darlegen, wie der EVG eindeutig identifiziert wird.**

Aufgaben des Evaluators

E1.17 **Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.**

Aspekt 2 - Programmiersprachen und Compiler

Anforderungen an Inhalt und Form

E1.18 **Keine Anforderungen.**

Anforderungen an Nachweise

E1.19 **Keine Anforderungen.**

Aufgaben des Evaluators

E1.20 **Keine Aufgaben.**

Aspekt 3 - Sicherheit beim Entwickler

Anforderungen an Inhalt und Form

E1.21 **Keine Anforderungen.**

Anforderungen an Nachweise

E1.22 **Keine Anforderungen.**

Aufgaben des Evaluators

E1.23 **Keine Aufgaben.**

Betrieb - Die Betriebsdokumentation

E1.24 Der Antragsteller muß die folgende Dokumentation bereitstellen:

- **Benutzerdokumentation**
- **Systemverwalter-Dokumentation**

Aspekt 1 - Benutzerdokumentation

Anforderungen an Inhalt und Form

E1.25 **Die Benutzerdokumentation muß die sicherheitsspezifischen Funktionen, die für den Endnutzer von Bedeutung sind, darlegen. Daneben muß sie auch Richtlinien für ihre sichere Anwendung enthalten. Die Benutzerdokumentation, zu welcher beispielsweise Referenz-Manuale, Benutzeranleitungen etc. gehören, muß strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.**

Anforderungen an Nachweise

E1.26 **Die Benutzerdokumentation muß darlegen, wie ein Endnutzer den EVG in einer sicheren Art und Weise nutzt.**

Aufgaben des Evaluators

E1.27 **Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.**

Aspekt 2 - Systemverwalter-Dokumentation

Anforderungen an Inhalt und Form

E1.28 **Die Systemverwalter-Dokumentation muß die sicherheitsspezifischen Funktionen darlegen, die für den Systemverwalter von Bedeutung sind. Sie muß zwei Funktionsarten unterscheiden: solche, mit denen der Systemverwalter die Sicherheitsparameter kontrollieren kann, und solche, mit denen er lediglich Informationen abfragen kann. Wenn ein Systemverwalter notwendig ist, muß sie alle Sicherheitsparameter darlegen, die er kontrollieren kann. Sie muß jeden Typ eines sicherheitsrelevanten Ereignisses darlegen, der für die Systemverwaltungsfunktionen von Bedeutung ist. Sie muß Details zu den Verfahren, die für die Sicherheitsadministration relevant sind, in einer Form darlegen, die für die Handhabung ausreichend ist. Sie muß Richtlinien zu der konsistenten und wirksamen Nutzung der Sicherheitseigenschaften des EVG enthalten und darlegen, wie solche Eigenschaften zusammenwirken. Sie muß die Anweisungen darlegen, wie das System/Produkt installiert wird und wie es, wenn erforderlich, konfiguriert wird. Die Systemverwalter-Dokumentation, z.B. Referenz-Manuale, Systemverwalter-Anleitungen etc., muß strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.**

Anforderungen an Nachweise

E1.29 **Die Systemverwalter-Dokumentation muß darlegen, wie der EVG sicher verwaltet wird.**

Aufgaben des Evaluators

E1.30 **Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.**

Betrieb - Die Betriebsumgebung

E1.31 Der Antragsteller hat die folgende Dokumentation bereitzustellen:

- **Auslieferungs- und Konfigurations-Dokumentation**
- **Anlauf- und Betriebs-Dokumentation**

Aspekt 1 - Auslieferung und Konfiguration

Anforderungen an Prozeduren und Standards

E1.32 **Wenn unterschiedliche Konfigurationen möglich sind, muß die Auswirkung der einzelnen Konfigurationen auf die Sicherheit dargelegt werden. Die Verfahren der Auslieferung und Systemgenerierung sind darzulegen.**

Anforderungen an Nachweise

E1.33 **Die vorgelegten Informationen müssen darlegen, wie die genannten Verfahren die Sicherheit aufrechterhalten.**

Aufgaben des Evaluators

E1.34 **Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.**

Aspekt 2 - Anlauf und Betrieb

Anforderungen an Prozeduren und Standards

E1.35 **Die Prozeduren für einen sicheren Anlauf und Betrieb müssen dargelegt werden.**

Anforderungen an Nachweise

E1.36 **Die vorgelegten Informationen müssen darlegen, wie die Prozeduren die Sicherheit aufrechterhalten.**

Aufgaben des Evaluators

E1.37 **Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.**

Stufe E2

Konstruktion - Der Entwicklungsprozeß

E2.1 Der Antragsteller muß den EVG und die folgende Dokumentation bereitstellen:

- Die Sicherheitsvorgaben für den EVG
- informelle Beschreibung der Architektur des EVG
- **informelle Beschreibung des Feinentwurfs**
- **Testdokumentation**
- **Bibliothek der Testprogramme und -werkzeuge, die für den Test des EVG benutzt wurden**

Phase 1 - Anforderungen

Anforderungen an Inhalt und Form

E2.2 Die Sicherheitsvorgaben müssen die sicherheitsspezifischen Funktionen darlegen, die vom EVG zur Verfügung gestellt werden. Im Falle eines Systems müssen die Sicherheitsvorgaben zusätzlich eine System-Sicherheitspolitik (SSP) enthalten, die die Sicherheitsziele und Bedrohungen des Systems identifiziert. Für ein Produkt müssen die Sicherheitsvorgaben zusätzliche Aussagen enthalten, die die Art des Produkteinsatzes, die vorgesehene Einsatzumgebung und die für diese Einsatzumgebung angenommenen Bedrohungen identifizieren. Die in den Sicherheitsvorgaben aufgeführten sicherheitsspezifischen Funktionen müssen in informeller Notation (siehe Kapitel 2) spezifiziert werden.

Anforderungen an Nachweise

E2.3 Im Falle eines Systems müssen die Sicherheitsvorgaben darlegen, auf welche Weise die vorgeschlagene Funktionalität die Sicherheitsziele erfüllt und wie sie den definierten Bedrohungen angemessen entgegenwirkt. Im Fall eines Produktes müssen die Sicherheitsvorgaben darlegen, warum die Funktionalität für diese Art des Einsatzes zweckmäßig ist und wie sie den angenommenen Bedrohungen entgegenwirkt.

Aufgaben des Evaluators

E2.4 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist zu überprüfen, ob es Inkonsistenzen innerhalb der Sicherheitsvorgaben gibt.

Phase 2 - Architekturentwurf

Anforderungen an Inhalt und Form

E2.5 Diese Beschreibung muß die grundsätzliche Struktur sowie alle externen Schnittstellen des EVG darlegen. Sie muß die Hard- und Firmware darlegen, die der EVG benötigt, und die Funktionalität der unterstützenden Schutzmechanismen angeben, die in dieser Hard- oder Firmware implementiert sind. **Sie muß die Aufteilung des EVG in sicherheitsspezifische und andere Komponenten darlegen.**

Anforderungen an Nachweise

E2.6 Die Beschreibung der Architektur muß darlegen, wie die sicherheitsspezifischen Funktionen der Sicherheitsvorgaben zur Verfügung gestellt werden. **Sie muß darlegen, wie die Trennung in sicherheitsspezifische und andere Komponenten erreicht wird.**

Aufgaben des Evaluators

E2.7 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. **Es ist zu überprüfen, ob die Trennung von sicherheitsspezifischen und anderen Komponenten wirksam ist.**

Phase 3 - Feinentwurf

Anforderungen an Inhalt und Form

E2.8 **Der Feinentwurf muß die Realisierung aller sicherheitsspezifischen und sicherheitsrelevanten Funktionen darlegen. Er muß alle Sicherheitsmechanismen identifizieren. Er muß die sicherheitsspezifischen Funktionen auf Mechanismen und Komponenten abbilden. Alle Schnittstellen der sicherheitsspezifischen und der sicherheitsrelevanten Komponenten müssen mit ihrem Zweck und ihren Parametern dokumentiert werden. Spezifikationen/Definitionen für die Mechanismen müssen zur Verfügung gestellt werden. Diese Spezifikationen müssen für die Analyse der Beziehungen zwischen den verwendeten Mechanismen geeignet sein. Für Komponenten, die weder sicherheitsspezifisch noch sicherheitsrelevant sind, müssen keine Spezifikationen zur Verfügung gestellt werden. Wo mehr als eine Spezifikationsebene vorliegt, muß eine klare und hierarchische Beziehung zwischen den Ebenen bestehen.**

Anforderung an Nachweise

E2.9 **Der Feinentwurf muß darlegen, auf welche Weise die Sicherheitsmechanismen die sicherheitsspezifischen Funktionen, die in den Sicherheitsvorgaben spezifiziert sind, realisieren. Er muß darlegen, warum Komponenten, für die keine Ent-**

wurfsunterlagen zur Verfügung gestellt werden, weder sicherheitsspezifisch noch sicherheitsrelevant sein können.

Aufgaben des Evaluators

E2.10 **Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.**

Phase 4 - Implementierung

Anforderungen an Inhalt und Form

E2.11 **Die Testdokumentation muß Testpläne, Testziele, Testverfahren und Testergebnisse enthalten. Die Bibliothek von Testprogrammen muß Testprogramme und -werkzeuge enthalten, mit denen alle Tests, die in der Testdokumentation beschrieben sind, wiederholt werden können.**

Anforderungen an Nachweise

E2.12 **Die Testdokumentation muß die Übereinstimmung zwischen den Tests und den in den Sicherheitsvorgaben definierten sicherheitsspezifischen Funktionen darlegen.**

Aufgaben des Evaluators

E2.13 **Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die Bibliothek der Testprogramme ist für eine stichprobenweise Überprüfung der Testergebnisse heranzuziehen. Es ist zu überprüfen, ob die Tests alle sicherheitsspezifischen Funktionen, die in den Sicherheitsvorgaben angegeben sind, umfassen. Zusätzlich sind Tests zur Fehlersuche durchzuführen.**

Konstruktion - Die Entwicklungsumgebung

E2.14 Der Antragsteller muß die folgende Dokumentation bereitstellen:

- Konfigurationsliste, die die Version des EVG für die Evaluation identifiziert
- **Informationen über das Konfigurationskontrollsystem**
- **Informationen über die Sicherheit der Entwicklungsumgebung**

Aspekt 1 - Konfigurationskontrolle

Anforderungen an Inhalt und Form

E2.15 **Der Entwicklungsvorgang muß durch ein Konfigurationskontrollsystem unterstützt werden. Die vorgelegte Konfigurationsliste muß alle Basiskomponenten auflisten, aus denen der EVG besteht. Der EVG, seine Basiskomponenten und alle zur Verfügung gestellten Dokumente, einschließlich der Handbücher, müssen eine eindeutige Identifikation besitzen. Die Verwendung dieser Identifikation bei Verweisen wird zwingend vorgeschrieben. Das Konfigurationskontrollsystem muß sicherstellen, daß der in Evaluation befindliche EVG mit der zur Verfügung gestellten Dokumentation übereinstimmt und daß nur autorisierte Änderungen möglich sind.**

Anforderungen an Nachweise

E2.16 **Die Informationen über das Konfigurationskontrollsystem müssen darlegen, wie es in der Praxis benutzt wird und wie es im Entwicklungsprozeß zusammen mit den Qualitätsmanagementverfahren des Herstellers angewendet wird.**

Aufgaben des Evaluators

E2.17 **Es ist zu überprüfen, ob die dokumentierten Verfahren angewendet werden.** Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Aspekt 2 - Programmiersprachen und Compiler

Anforderungen an Inhalt und Form

E2.18 Keine Anforderungen.

Anforderungen an Nachweise

E2.19 Keine Anforderungen.

Aufgaben des Evaluators

E2.20 Keine Anforderungen.

Aspekt 3 - Sicherheit beim Entwickler

Anforderungen an Inhalt und Form

E2.21 **Das Dokument über die Sicherheit der Entwicklungsumgebung muß die geplanten Schutzmaßnahmen bzgl. der Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumente darlegen. Materielle, organisatorische, personelle und andere Sicherheitsmaßnahmen, die durch den Entwickler eingesetzt werden, müssen dargelegt werden.**

Anforderungen an Nachweise

E2.22 **Die Information über die Sicherheit der Entwicklungsumgebung muß darlegen, wie die Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumentation gewährleistet werden.**

Aufgaben des Evaluators

E2.23 **Es ist zu überprüfen, ob die dokumentierten Verfahren angewendet werden. Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist nach Fehlern in den Verfahren zu suchen.**

Betrieb - Die Betriebsdokumentation

E2.24 Der Antragsteller muß die folgende Dokumentation bereitstellen:

- Benutzerdokumentation
- Systemverwalter-Dokumentation

Aspekt 1 - Benutzerdokumentation

Anforderungen an Inhalt und Form

E2.25 Die Benutzerdokumentation muß die sicherheitsspezifischen Funktionen, die für den Endnutzer von Bedeutung sind, darlegen. Daneben muß sie auch Richtlinien für ihre sichere Anwendung enthalten. Die Benutzerdokumentation, zu welcher beispielsweise Referenz-Manuale, Benutzeranleitungen etc. gehören, muß strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.

Anforderungen an Nachweise

E2.26 Die Benutzerdokumentation muß darlegen, wie ein Endnutzer den EVG in einer sicheren Art und Weise nutzt.

Aufgaben des Evaluators

E2.27 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Aspekt 2 - Systemverwalter-Dokumentation

Anforderungen an Inhalt und Form

E2.28 Die Systemverwalter-Dokumentation muß die sicherheitsspezifischen Funktionen darlegen, die für den Systemverwalter von Bedeutung sind. Sie muß zwei Funktionsarten unterscheiden: solche, mit denen der Systemverwalter die Sicherheitsparameter kontrollieren kann, und solche, mit denen er lediglich Informationen abfragen kann. Wenn ein Systemverwalter notwendig ist, muß sie alle Sicherheitsparameter darlegen, die er kontrollieren kann. Sie muß jeden Typ eines sicherheitsrelevanten Ereignisses darlegen, der für die Systemverwaltungsfunktionen von Bedeutung ist. Sie muß Details zu den Verfahren, die für die Sicherheitsadministration relevant sind, in einer Form darlegen, die für die Handhabung ausreichend ist. Sie muß Richtlinien zu der konsistenten und wirksamen Nutzung der Sicherheitseigenschaften des EVG enthalten und darlegen, wie solche Eigenschaften zusammenwirken. Sie muß die Anweisungen darlegen, wie das System/Produkt installiert wird und wie es, wenn erforderlich, konfiguriert wird. Die Systemverwalter-Dokumentation, z.B. Referenz-Manuale, Systemverwalter-Anleitungen etc., muß strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.

Anforderungen an Nachweise

E2.29 Die Systemverwalter-Dokumentation muß darlegen, wie der EVG sicher verwaltet wird.

Aufgaben des Evaluators

E2.30 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Betrieb - Die Betriebsumgebung

E2.31 Der Antragsteller hat die folgende Dokumentation bereitzustellen:

- Auslieferungs- und Konfigurations-Dokumentation
- Anlauf- und Betriebs-Dokumentation

Aspekt 1 - Auslieferung und Konfiguration

Anforderungen an Prozeduren und Standards

E2.32 Wenn unterschiedliche Konfigurationen möglich sind, muß die Auswirkung der einzelnen Konfigurationen auf die Sicherheit dargelegt werden. Die Verfahren der Auslieferung und Systemgenerierung sind darzulegen. **Ein von der nationalen Zertifizierungsbehörde für diese Stufe zugelassenes Verfahren muß angewendet werden, welches die Authentizität des ausgelieferten EVG garantiert. Bei der Generierung des EVG müssen alle Generierungsoptionen und/oder Änderungen so protokolliert werden, daß es später möglich ist, exakt zu rekonstruieren wie und wann der EVG generiert wurde.**

Anforderungen an Nachweise

E2.33 Die vorgelegten Informationen müssen darlegen, wie die genannten Verfahren die Sicherheit aufrechterhalten.

Aufgaben des Evaluators

E2.34 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. **Die korrekte Anwendung der Auslieferungsverfahren ist zu überprüfen. Es ist nach Fehlern in den Verfahren zur Systemgenerierung zu suchen.**

Aspekt 2 - Anlauf und Betrieb

Anforderungen an Prozeduren und Standards

E2.35 Die Prozeduren für einen sicheren Anlauf und Betrieb müssen dargelegt werden. **Wenn irgendwelche sicherheitsspezifischen Funktionen während des Anlaufs, des normalen Betriebes oder der Wartung ausgeschaltet oder modifiziert werden können, so muß dies dargelegt werden. Wenn der EVG sicherheitsspezifische Hardware-Komponenten enthält, dann müssen hierfür Diagnoseeinrichtungen vorhanden sein, die durch den Systemverwalter, den Benutzer oder selbsttätig in der Einsatzumgebung aktiviert werden können.**

Anforderungen an Nachweise

E2.36 Die vorgelegten Informationen müssen darlegen, wie die Prozeduren die Sicherheit aufrechterhalten. **Der Antragsteller muß Beispiele von Ergebnissen aller Diagnoseprozeduren der in Hardware implementierten sicherheitsspezifischen Komponenten zur Verfügung stellen. Der Antragsteller muß Beispiele aller Protokollaufzeichnungen vorlegen, die während des Anlaufs und des Betriebes erstellt werden.**

Aufgaben des Evaluators

E2.37 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. **Die beispielhaften Nachweise für den Anlauf und den Betrieb sind zu überprüfen. Es ist nach Fehlern in den Prozeduren zu suchen.**

Stufe E3

Konstruktion - Der Entwicklungsprozeß

E3.1 Der Antragsteller muß den EVG und die folgende Dokumentation bereitstellen:

- Die Sicherheitsvorgaben für den EVG
- informelle Beschreibung der Architektur des EVG
- informelle Beschreibung des Feinentwurfs
- Testdokumentation
- Bibliothek der Testprogramme und -werkzeuge, die für den Test des EVG benutzt wurden
- **Quellcode bzw. Hardware-Konstruktionszeichnungen für alle sicherheitsspezifischen und sicherheitsrelevanten Komponenten**
- **informelle Zuordnungsbeschreibung, die den Bezug zwischen Quellcode bzw. Hardware-Konstruktionszeichnungen und dem Feinentwurf darstellt**

Phase 1 - Anforderungen

Anforderungen an Inhalt und Form

E3.2 Die Sicherheitsvorgaben müssen die sicherheitsspezifischen Funktionen **beschreiben**, die vom EVG zur Verfügung gestellt werden. Im Falle eines Systems müssen die Sicherheitsvorgaben zusätzlich eine System-Sicherheitspolitik (SSP) enthalten, die die Sicherheitsziele und Bedrohungen des Systems identifiziert. Für ein Produkt müssen die Sicherheitsvorgaben zusätzliche Aussagen enthalten, die die Art des Produkteinsatzes, die vorgesehene Einsatzumgebung und die für diese Einsatzumgebung angenommenen Bedrohungen identifizieren. Die in den Sicherheitsvorgaben aufgeführten sicherheitsspezifischen Funktionen müssen in informeller Notation (siehe Kapitel 2) spezifiziert werden.

Anforderungen an Nachweise

E3.3 Im Falle eines Systems müssen die Sicherheitsvorgaben **beschreiben**, auf welche Weise die vorgeschlagene Funktionalität die Sicherheitsziele erfüllt und wie sie den definierten Bedrohungen angemessen entgegenwirkt. Im Fall eines Produktes müssen

die Sicherheitsvorgaben **beschreiben**, warum die Funktionalität für diese Art des Einsatzes zweckmäßig ist und wie sie den angenommenen Bedrohungen entgegenwirkt.

Aufgaben des Evaluators

E3.4 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist zu überprüfen, ob es Inkonsistenzen innerhalb der Sicherheitsvorgaben gibt.

Phase 2 - Architekturentwurf

Anforderungen an Inhalt und Form

E3.5 Diese Beschreibung muß die grundsätzliche Struktur sowie alle externen Schnittstellen des EVG **beschreiben**. Sie muß die Hard- und Firmware **beschreiben**, die der EVG benötigt, und die Funktionalität der unterstützenden Schutzmechanismen angeben, die in dieser Hard- oder Firmware implementiert sind. Sie muß die Aufteilung des EVG in sicherheitsspezifische und andere Komponenten **beschreiben**.

Anforderungen an Nachweise

E3.6 Die Beschreibung der Architektur muß **beschreiben**, wie die sicherheitsspezifischen Funktionen der Sicherheitsvorgaben zur Verfügung gestellt werden. Sie muß **beschreiben**, wie die Trennung in sicherheitsspezifische und andere Komponenten erreicht wird.

Aufgaben des Evaluators

E3.7 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist zu überprüfen, ob die Trennung von sicherheitsspezifischen und anderen Komponenten wirksam ist.

Phase 3 - Feinentwurf

Anforderungen an Inhalt und Form

E3.8 **Der Feinentwurf muß alle Basiskomponenten spezifizieren.** Er muß die Realisierung aller sicherheitsspezifischen und sicherheitsrelevanten Funktionen **beschreiben**. Er muß alle Sicherheitsmechanismen identifizieren. Er muß die sicherheitsspezifischen Funktionen auf Mechanismen und Komponenten abbilden. Alle Schnittstellen der sicherheitsspezifischen und der sicherheitsrelevanten Komponenten müssen mit ihrem Zweck und ihren Parametern dokumentiert werden. Spezifikationen/Definitionen für die Mechanismen müssen zur Verfügung gestellt werden. Diese Spezifikationen müssen für die Analyse der Beziehungen zwischen den verwendeten Mechanismen geeignet sein. Für Komponenten, die weder sicherheitsspezifisch noch sicherheitsrelevant sind, müssen

keine Spezifikationen zur Verfügung gestellt werden. Wo mehr als eine Spezifikationsebene vorliegt, muß eine klare und hierarchische Beziehung zwischen den Ebenen bestehen.

Anforderung an Nachweise

E3.9 Der Feinentwurf muß **beschreiben**, auf welche Weise die Sicherheitsmechanismen die sicherheitsspezifischen Funktionen, die in den Sicherheitsvorgaben spezifiziert sind, realisieren. Er muß **beschreiben**, warum Komponenten, für die keine Entwurfsunterlagen zur Verfügung gestellt werden, weder sicherheitsspezifisch noch sicherheitsrelevant sein können.

Aufgaben des Evaluators

E3.10 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Phase 4 - Implementierung

Anforderungen an Inhalt und Form

E3.11 **Die Zuordnungsbeschreibung muß die Übereinstimmung zwischen Quellcode bzw. Hardware-Konstruktionszeichnungen und den Basiskomponenten des Feinentwurfs beschreiben**. Die Testdokumentation muß Testpläne, Testziele, Testverfahren und Testergebnisse enthalten. Die Bibliothek von Testprogrammen muß Testprogramme und -werkzeuge enthalten, mit denen alle Tests, die in der Testdokumentation beschrieben sind, wiederholt werden können.

Anforderungen an Nachweise

E3.12 Die Testdokumentation muß die Übereinstimmung zwischen den Tests und den in den Sicherheitsvorgaben definierten sicherheitsspezifischen Funktionen **beschreiben**. **Sie muß die Übereinstimmung zwischen den Tests und den sicherheitsspezifischen und sicherheitsrelevanten Funktionen beschreiben, die im Feinentwurf definiert sind. Sie muß die Übereinstimmung zwischen den Tests und den Sicherheitsmechanismen beschreiben, wie sie im Quellcode bzw. in den Hardware-Konstruktionszeichnungen dargestellt sind. Nachweise über Wiederholungstests nach der Entdeckung und Korrektur sicherheitsrelevanter Fehler sind zwingend, um zu zeigen, daß die Fehler behoben wurden und daß keine neuen Fehler eingefügt wurden.**

Aufgaben des Evaluators

E3.13 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die Bibliothek der Testprogramme ist für eine stichprobenweise Überprüfung der Testergebnisse heranzuziehen. Es ist zu überprüfen, ob die Tests alle sicherheitsspezifischen Funktionen, die in den Sicherheitsvorgaben angegeben sind, umfassen. **Es ist zu überprüfen, ob die Tests alle im Feinentwurf identifizierten sicherheitsspezifischen und sicherheitsrelevanten Funktionen sowie alle im Quellcode bzw. in den Hardware-Konstruktionszeichnungen identifizierbaren Sicherheitsmechanismen umfassen. Alle Wiederholungstests, die auf die Fehlerkorrektur erfolgten, sind zu überprüfen.** Zusätzlich sind Tests zur Fehlersuche durchzuführen.

Konstruktion - Die Entwicklungsumgebung

E3.14 Der Antragsteller muß die folgende Dokumentation bereitstellen:

- Konfigurationsliste, die die Version des EVG für die Evaluation identifiziert
- Informationen über das Konfigurationskontrollsystem
- **Informationen über das Abnahmeverfahren**
- Informationen über die Sicherheit der Entwicklungsumgebung
- **Beschreibung aller benutzten Implementierungssprachen**

Aspekt 1 - Konfigurationskontrolle

Anforderungen an Inhalt und Form

E3.15 Der Entwicklungsvorgang muß durch ein Konfigurationskontrollsystem **und Abnahmeverfahren** unterstützt werden. Die vorgelegte Konfigurationsliste muß alle Basiskomponenten auflisten, aus denen der EVG besteht. Der EVG, seine Basiskomponenten und alle zur Verfügung gestellten Dokumente, einschließlich der Handbücher **und des Quellcodes bzw. der Hardware-Konstruktionszeichnungen,** müssen eine eindeutige Identifikation besitzen. Die Verwendung dieser Identifikation bei Verweisen wird zwingend vorgeschrieben. Das Konfigurationskontrollsystem muß sicherstellen, daß der in Evaluation befindliche EVG mit der zur Verfügung gestellten Dokumentation übereinstimmt und daß nur autorisierte Änderungen möglich sind.

Anforderungen an Nachweise

E3.16 Die Informationen über das Konfigurationskontrollsystem müssen **beschreiben**, wie es in der Praxis benutzt wird und wie es im Entwicklungsprozeß zusammen mit den Qualitätsmanagementverfahren des Herstellers angewendet wird.

Aufgaben des Evaluators

E3.17 Es ist zu überprüfen, ob die dokumentierten Verfahren angewendet werden. Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Aspekt 2 - Programmiersprachen und Compiler

Anforderungen an Inhalt und Form

E3.18 **Alle Programmiersprachen, die für die Implementierung benutzt werden, müssen klar definiert sein, wie z.B. in einem ISO-Standard. Alle implementierungsabhängigen Optionen der Programmiersprache müssen dokumentiert sein.**

Anforderungen an Nachweise

E3.19 **Die Definition der jeweiligen Programmiersprache muß die Bedeutung aller Anweisungen, die im Quellcode benutzt werden, eindeutig festlegen.**

Aufgaben des Evaluators

E3.20 **Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.**

Aspekt 3 - Sicherheit beim Entwickler

Anforderungen an Inhalt und Form

E3.21 Das Dokument über die Sicherheit der Entwicklungsumgebung muß die geplanten Schutzmaßnahmen bzgl. der Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumente **beschreiben**. Materielle, organisatorische, personelle und andere Sicherheitsmaßnahmen, die durch den Entwickler eingesetzt werden, müssen **beschrieben** werden.

Anforderungen an Nachweise

E3.22 Die Information über die Sicherheit der Entwicklungsumgebung muß **beschreiben**, wie die Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumentation gewährleistet werden.

Aufgaben des Evaluators

E3.23 Es ist zu überprüfen, ob die dokumentierten Verfahren angewendet werden. Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist nach Fehlern in den Verfahren zu suchen.

Betrieb - Die Betriebsdokumentation

E3.24 Der Antragsteller muß die folgende Dokumentation bereitstellen:

- Benutzerdokumentation
- Systemverwalter-Dokumentation

Aspekt 1 - Benutzerdokumentation

Anforderungen an Inhalt und Form

E3.25 Die Benutzerdokumentation muß die sicherheitsspezifischen Funktionen, die für den Endnutzer von Bedeutung sind, **beschreiben**. Daneben muß sie auch Richtlinien für ihre sichere Anwendung enthalten. Die Benutzerdokumentation, zu welcher beispielsweise Referenz-Manuale, Benutzeranleitungen etc. gehören, muß strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.

Anforderungen an Nachweise

E3.26 Die Benutzerdokumentation muß **beschreiben**, wie ein Endnutzer den EVG in einer sicheren Art und Weise nutzt.

Aufgaben des Evaluators

E3.27 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Aspekt 2 - Systemverwalter-Dokumentation

Anforderungen an Inhalt und Form

E3.28 Die Systemverwalter-Dokumentation muß die sicherheitsspezifischen Funktionen **beschreiben**, die für den Systemverwalter von Bedeutung sind. Sie muß zwei Funktionsarten unterscheiden: solche, mit denen der Systemverwalter die Sicherheitsparameter kontrollieren kann, und solche, mit denen er lediglich Informationen abfragen kann. Wenn ein Systemverwalter notwendig ist, muß sie alle Sicherheitsparameter **beschreiben**, die er kontrollieren kann. Sie muß jeden Typ eines sicherheitsrelevanten Ereignisses **beschreiben**, der für die Systemverwaltungsfunktionen von Bedeutung ist. Sie muß Details zu den Verfahren, die für die Sicherheitsadministration relevant sind, in einer Form **beschreiben**, die für die Handhabung ausreichend ist. Sie muß Richtlinien zu der konsistenten und wirksamen Nutzung der Sicherheitseigenschaften des EVG enthalten und beschreiben, wie solche Eigenschaften zusammenwirken. Sie muß die Anweisungen **beschreiben**, wie das System/Produkt installiert wird und wie es, wenn erforderlich, konfiguriert wird. Die Systemverwalter-Dokumentation, z.B. Referenz-Manuale, Systemverwalter-Anleitungen etc., muß strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.

Anforderungen an Nachweise

E3.29 Die Systemverwalter-Dokumentation muß **beschreiben**, wie der EVG sicher verwaltet wird.

Aufgaben des Evaluators

E3.30 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Betrieb - Die Betriebsumgebung

E3.31 Der Antragsteller hat die folgende Dokumentation bereitzustellen:

- Auslieferungs- und Konfigurations-Dokumentation
- Anlauf- und Betriebs-Dokumentation

Aspekt 1 - Auslieferung und Konfiguration

Anforderungen an Prozeduren und Standards

E3.32 Wenn unterschiedliche Konfigurationen möglich sind, muß die Auswirkung der einzelnen Konfigurationen auf die Sicherheit **beschrieben** werden. Die Verfahren der Auslieferung und Systemgenerierung sind zu **beschreiben**. Ein von der nationalen Zertifizierungsbehörde für diese Stufe zugelassenes Verfahren muß angewendet werden, welches die Authentizität des ausgelieferten EVG garantiert. Bei der Generierung des EVG müssen alle Generierungsoptionen und/oder Änderungen so protokolliert werden, daß es später möglich ist, exakt zu rekonstruieren wie und wann der EVG generiert wurde.

Anforderungen an Nachweise

E3.33 Die vorgelegten Informationen müssen **beschreiben**, wie die genannten Verfahren die Sicherheit aufrechterhalten.

Aufgaben des Evaluators

E3.34 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die korrekte Anwendung der Auslieferungsverfahren ist zu überprüfen. Es ist nach Fehlern in den Verfahren zur Systemgenerierung zu suchen.

Aspekt 2 - Anlauf und Betrieb

Anforderungen an Prozeduren und Standards

E3.35 Die Prozeduren für einen sicheren Anlauf und Betrieb müssen **beschrieben** werden. Wenn irgendwelche sicherheitsspezifische Funktionen während des Anlaufs, des normalen Betriebes oder der Wartung ausgeschaltet oder modifiziert werden können, so muß dies **beschrieben** werden. Wenn der EVG sicherheitsspezifische Hardware-Komponenten enthält, dann müssen hierfür Diagnoseeinrichtungen vorhanden sein, die durch den Administrator, den Benutzer oder selbsttätig in der Einsatzumgebung aktiviert werden können.

Anforderungen an Nachweise

E3.36 Die vorgelegten Informationen müssen **beschreiben**, wie die Prozeduren die Sicherheit aufrechterhalten. Der Antragsteller muß Beispiele von Ergebnissen aller Diagnoseprozeduren der in Hardware implementierten sicherheitsspezifischen Komponenten zur Verfügung stellen. Der Antragsteller muß Beispiele aller Protokollaufzeichnungen vorlegen, die während des Anlaufs und des Betriebes erstellt werden.

Aufgaben des Evaluators

E3.37 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die beispielhaften Nachweise für den Anlauf und den Betrieb sind zu überprüfen. Es ist nach Fehlern in den Prozeduren zu suchen.

Stufe E4

Konstruktion - Der Entwicklungsprozeß

E4.1 Der Antragsteller muß den EVG und die folgende Dokumentation bereitstellen:

- Die Sicherheitsvorgaben für den EVG
- **Definition eines zugrundeliegenden formal spezifizierten Sicherheitsmodells oder Verweis auf ein solches**
- **informelle Interpretation des zugrundeliegenden Modells bezüglich der Sicherheitsvorgaben**
- **semiformale** Beschreibung der Architektur des EVG
- **semiformale** Beschreibung des Feinentwurfs
- Testdokumentation
- Bibliothek der Testprogramme und -werkzeuge, die für den Test des EVG benutzt wurden
- Quellcode bzw. Hardware-Konstruktionszeichnungen für alle sicherheitsspezifischen und sicherheitsrelevanten Komponenten
- informelle Zuordnungsbeschreibung, die den Bezug zwischen Quellcode bzw. Hardware-Konstruktionszeichnungen und dem Feinentwurf darstellt

Phase 1 - Anforderungen

Anforderungen an Inhalt und Form

E4.2 Die Sicherheitsvorgaben müssen die sicherheitsspezifischen Funktionen beschreiben, die vom EVG zur Verfügung gestellt werden. Im Falle eines Systems müssen die Sicherheitsvorgaben zusätzlich eine System-Sicherheitspolitik (SSP) enthalten, die die Sicherheitsziele und Bedrohungen des Systems identifiziert. Für ein Produkt müssen die Sicherheitsvorgaben zusätzliche Aussagen enthalten, die die Art des Produkteinsatzes, die vorgesehene Einsatzumgebung und die für diese Einsatzumgebung angenommenen Bedrohungen identifizieren. **Ein formales Sicherheitsmodell oder ein Verweis auf ein solches muß zur Verfügung gestellt werden. Darin ist die zugrundeliegende Sicherheitspolitik zu definieren, die vom EVG durchgesetzt werden muß. Eine informelle Interpretation dieses Modells in Bezug zu den Sicherheitsvorgaben muß zur Verfügung gestellt werden.** Die in den Sicherheitsvorgaben aufgeführten sicherheitsspezifischen Funktionen müssen **sowohl** in informeller **als auch in semiformaler** Notation (siehe Kapitel 2) spezifiziert werden.

Anforderungen an Nachweise

E4.3 Im Falle eines Systems müssen die Sicherheitsvorgaben beschreiben, auf welche Weise die vorgeschlagene Funktionalität die Sicherheitsziele erfüllt und wie sie den definierten Bedrohungen angemessen entgegenwirkt. Im Fall eines Produktes müssen die Sicherheitsvorgaben beschreiben, warum die Funktionalität für diese Art des Einsatzes zweckmäßig ist und wie sie den angenommenen Bedrohungen entgegenwirkt. **Die informelle Interpretation des formalen Sicherheitsmodells muß beschreiben, auf welche Weise seine zugrundeliegende Sicherheitspolitik durch die Sicherheitsvorgaben erfüllt wird.**

Aufgaben des Evaluators

E4.4 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist zu überprüfen, ob es Inkonsistenzen innerhalb der Sicherheitsvorgaben gibt. **Es ist zu überprüfen, ob es Sicherheitsmaßnahmen in den Sicherheitsvorgaben gibt, die zu Konflikten mit der dem Sicherheitsmodell zugrundeliegenden Sicherheitspolitik führen.**

Phase 2 - Architekturentwurf

Anforderungen an Inhalt und Form

E4.5 **Eine semiformale Notation muß verwendet werden, um einen semiformalen Architekturentwurf zu erstellen.** Diese Beschreibung muß die grundsätzliche Struktur sowie alle externen Schnittstellen des EVG beschreiben. Sie muß die Hard- und Firmware beschreiben, die der EVG benötigt, und die Funktionalität der unterstützenden Schutzmechanismen angeben, die in dieser Hard- oder Firmware implementiert sind. Sie muß die Aufteilung des EVG in sicherheitsspezifische und andere Komponenten beschreiben.

Anforderungen an Nachweise

E4.6 Die Beschreibung der Architektur muß beschreiben, wie die sicherheitsspezifischen Funktionen der Sicherheitsvorgaben zur Verfügung gestellt werden. Sie muß beschreiben, wie die Trennung in sicherheitsspezifische und andere Komponenten erreicht wird. **Sie muß beschreiben, auf welche Weise die gewählte Struktur die größtmögliche Unabhängigkeit der sicherheitsspezifischen Komponenten gewährleistet.**

Aufgaben des Evaluators

E4.7 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist zu überprüfen, ob die Trennung von sicherheitsspezifischen und anderen Komponenten wirksam ist.

Phase 3 - Feinentwurf

Anforderungen an Inhalt und Form

E4.8 **Eine semiformale Notation muß verwendet werden, um einen semiformalen Feinentwurf zu erstellen.** Der Feinentwurf muß alle Basiskomponenten spezifizieren. **Er muß durch alle Ebenen der Entwurfshierarchie die Realisierung aller sicherheitsspezifischen und aller sicherheitsrelevanten Funktionen beschreiben. Er muß die Aufteilung des EVG in sicherheitsspezifische, sicherheitsrelevante und in andere Komponenten beschreiben. Er muß in klar definierte, weitgehend voneinander unabhängige Basiskomponenten aufgegliedert sein, die das Testen erleichtern und die Möglichkeiten zu einer Verletzung der Sicherheit minimieren.** Er muß alle Sicherheitsmechanismen identifizieren. Er muß die sicherheitsspezifischen Funktionen auf Mechanismen und Komponenten abbilden. Alle Schnittstellen der sicherheitsspezifischen und der sicherheitsrelevanten Komponenten müssen mit ihrem Zweck und ihren Parametern dokumentiert werden. Spezifikationen/Definitionen für die Mechanismen müssen zur Verfügung gestellt werden. Diese Spezifikationen müssen für die Analyse der Beziehungen zwischen den verwendeten Mechanismen geeignet sein. Für Komponenten, die weder sicherheitsspezifisch noch sicherheitsrelevant sind, müssen keine Spezifikationen zur Verfügung gestellt werden. Wo mehr als eine Spezifikationsebene vorliegt, muß eine klare und hierarchische Beziehung zwischen den Ebenen bestehen.

Anforderung an Nachweise

E4.9 Der Feinentwurf muß beschreiben, auf welche Weise die Sicherheitsmechanismen die sicherheitsspezifischen Funktionen, die in den Sicherheitsvorgaben spezifiziert sind, realisieren. Er muß beschreiben, warum Komponenten, für die keine Entwurfsunterlagen zur Verfügung gestellt werden, weder sicherheitsspezifisch noch sicherheitsrelevant sein können.

Aufgaben des Evaluators

E4.10 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Phase 4 - Implementierung

Anforderungen an Inhalt und Form

E4.11 Die Zuordnungsbeschreibung muß die Übereinstimmung zwischen Quellcode bzw. Hardware-Konstruktionszeichnungen und den Basiskomponenten des Feinentwurfs beschreiben. Die Testdokumentation muß Testpläne, Testziele, Testverfahren und Testergebnisse enthalten **und eine Begründung, warum die gewählte Testabdeckung ausreicht.** Die Bibliothek von Testprogrammen muß Testprogramme und -werkzeuge enthalten, mit denen alle Tests, die in der Testdokumentation beschrieben sind, wiederholt werden können.

Anforderungen an Nachweise

E4.12 Die Testdokumentation muß die Übereinstimmung zwischen den Tests und den in den Sicherheitsvorgaben definierten sicherheitsspezifischen Funktionen beschreiben. Sie muß die Übereinstimmung zwischen den Tests und den sicherheitsspezifischen und sicherheitsrelevanten Funktionen beschreiben, die im Feinentwurf definiert sind. Sie muß die Übereinstimmung zwischen den Tests und den Sicherheitsmechanismen beschreiben, wie sie im Quellcode bzw. in den Hardware-Konstruktionszeichnungen dargestellt sind. Nachweise über Wiederholungstests nach der Entdeckung und Korrektur sicherheitsrelevanter Fehler sind zwingend, um zu zeigen, daß die Fehler behoben wurden und daß keine neuen Fehler eingefügt wurden.

Aufgaben des Evaluators

E4.13 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die Bibliothek der Testprogramme ist für eine stichprobenweise Überprüfung der Testergebnisse heranzuziehen. Es ist zu überprüfen, ob die Tests alle sicherheitsspezifischen Funktionen, die in den Sicherheitsvorgaben angegeben sind, umfassen. Es ist zu überprüfen, ob die Tests alle im Feinentwurf identifizierten sicherheitsspezifischen und sicherheitsrelevanten Funktionen sowie alle im Quellcode bzw. in den Hardware-Konstruktionszeichnungen identifizierbaren Sicherheitsmechanismen umfassen. Alle Wiederholungstests, die auf die Fehlerkorrektur erfolgten, sind zu überprüfen. Zusätzlich sind Tests zur Fehlersuche durchzuführen.

Konstruktion - Die Entwicklungsumgebung

E4.14 Der Antragsteller muß die folgende Dokumentation bereitstellen:

- Konfigurationsliste, die die Version des EVG für die Evaluation identifiziert
- Informationen über das Konfigurationskontrollsystem **und seine Werkzeuge**
- **Protokollinformationen über Änderungen aller Teile des EVG, die der Konfigurationskontrolle unterliegen**

- Informationen über das Abnahmeverfahren
- Informationen über die Sicherheit der Entwicklungsumgebung
- Beschreibung aller benutzten Implementierungssprachen **und Compiler**

Aspekt 1 - Konfigurationskontrolle

Anforderungen an Inhalt und Form

E4.15 Der Entwicklungsvorgang muß durch ein, **durch Werkzeuge unterstütztes,** Konfigurationskontrollsystem und Abnahmeverfahren unterstützt werden. Die vorgelegte Konfigurationsliste muß alle Basiskomponenten auflisten, aus denen der EVG besteht. Der EVG, seine Basiskomponenten und alle zur Verfügung gestellten Dokumente, einschließlich der Handbücher und des Quellcodes bzw. der Hardware-Konstruktionszeichnungen, müssen eine eindeutige Identifikation besitzen. Die Verwendung dieser Identifikation bei Verweisen wird zwingend vorgeschrieben. Das Konfigurationskontrollsystem muß sicherstellen, daß der in Evaluation befindliche EVG mit der zur Verfügung gestellten Dokumentation übereinstimmt und daß nur autorisierte Änderungen **durch autorisierte Personen** möglich sind. **Die Werkzeuge des Konfigurationskontrollsystems müssen in der Lage sein, Änderungen zwischen unterschiedlichen Versionen von Objekten, die der Konfigurationskontrolle unterworfen sind, zu überwachen und zu protokollieren.**

Anforderungen an Nachweise

E4.16 Die Informationen über das Konfigurationskontrollsystem müssen beschreiben, wie es in der Praxis benutzt wird und wie es im Entwicklungsprozeß zusammen mit den Qualitätsmanagementverfahren des Herstellers angewendet wird.

Aufgaben des Evaluators

E4.17 Es ist zu überprüfen, ob die dokumentierten Verfahren angewendet werden. Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. **Ausgewählte Teile des EVG sind unter Verwendung der Werkzeuge des Entwicklers neu zu montieren; die Ergebnisse sind mit dem vorliegenden EVG zu vergleichen.**

Aspekt 2 - Programmiersprachen und Compiler

Anforderungen an Inhalt und Form

E4.18 Alle Programmiersprachen, die für die Implementierung benutzt werden, müssen klar definiert sein, wie z.B. in einem ISO-Standard. Alle implementierungsabhängigen

Optionen der Programmiersprache müssen dokumentiert sein. **Für alle benutzten Compiler müssen die gewählten Implementierungsoptionen dokumentiert werden.**

Anforderungen an Nachweise

E4.19 Die Definition der jeweiligen Programmiersprache muß die Bedeutung aller Anweisungen, die im Quellcode benutzt werden, eindeutig festlegen.

Aufgaben des Evaluators

E4.20 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Aspekt 3 - Sicherheit beim Entwickler

Anforderungen an Inhalt und Form

E4.21 Das Dokument über die Sicherheit der Entwicklungsumgebung muß die geplanten Schutzmaßnahmen bzgl. der Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumente darlegen. Materielle, organisatorische, personelle und andere Sicherheitsmaßnahmen, die durch den Entwickler eingesetzt werden, müssen beschrieben werden.

Anforderungen an Nachweise

E4.22 Die Information über die Sicherheit der Entwicklungsumgebung muß beschreiben, wie die Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumentation gewährleistet werden.

Aufgaben des Evaluators

E4.23 Es ist zu überprüfen, ob die dokumentierten Verfahren angewendet werden. Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist nach Fehlern in den Verfahren zu suchen.

Betrieb - Die Betriebsdokumentation

E4.24 Der Antragsteller muß die folgende Dokumentation bereitstellen:

- Benutzerdokumentation
- Systemverwalter-Dokumentation

Aspekt 1 - Benutzerdokumentation

Anforderungen an Inhalt und Form

E4.25 Die Benutzerdokumentation muß die sicherheitsspezifischen Funktionen, die für den Endnutzer von Bedeutung sind, beschreiben. Daneben muß sie auch Richtlinien für ihre sichere Anwendung enthalten. Die Benutzerdokumentation, zu welcher beispielsweise Referenz-Manuale, Benutzeranleitungen etc. gehören, muß strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.

Anforderungen an Nachweise

E4.26 Die Benutzerdokumentation muß beschreiben, wie ein Endnutzer den EVG in einer sicheren Art und Weise nutzt.

Aufgaben des Evaluators

E4.27 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Aspekt 2 - Systemverwalter-Dokumentation

Anforderungen an Inhalt und Form

E4.28 Die Systemverwalter-Dokumentation muß die sicherheitsspezifischen Funktionen beschreiben, die für den Systemverwalter von Bedeutung sind. Sie muß zwei Funktionsarten unterscheiden: solche, mit denen der Systemverwalter die Sicherheitsparameter kontrollieren kann, und solche, mit denen er lediglich Informationen abfragen kann. Wenn ein Systemverwalter notwendig ist, muß sie alle Sicherheitsparameter beschreiben, die er kontrollieren kann. Sie muß jeden Typ eines sicherheitsrelevanten Ereignisses beschreiben, der für die Systemverwaltungsfunktionen von Bedeutung ist. Sie muß Details zu den Verfahren, die für die Sicherheitsadministration relevant sind, in einer Form beschreiben, die für die Handhabung ausreichend ist. Sie muß Richtlinien zu der konsistenten und wirksamen Nutzung der Sicherheitseigenschaften des EVG enthalten und beschreiben, wie solche Eigenschaften zusammenwirken. Sie muß die Anweisungen beschreiben, wie das System/Produkt installiert wird und wie es, wenn

erforderlich, konfiguriert wird. Die Systemverwalter-Dokumentation, z.B. Referenz-Manuale, Systemverwalter-Anleitungen etc., muß strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.

Anforderungen an Nachweise

E4.29 Die Systemverwalter-Dokumentation muß beschreiben, wie der EVG sicher verwaltet wird.

Aufgaben des Evaluators

E4.30 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Betrieb - Die Betriebsumgebung

E4.31 Der Antragsteller hat die folgende Dokumentation bereitzustellen:

- Auslieferungs- und Konfigurations-Dokumentation
- Anlauf- und Betriebs-Dokumentation

Aspekt 1 - Auslieferung und Konfiguration

Anforderungen an Prozeduren und Standards

E4.32 Wenn unterschiedliche Konfigurationen möglich sind, muß die Auswirkung der einzelnen Konfigurationen auf die Sicherheit beschrieben werden. Die Verfahren der Auslieferung und Systemgenerierung sind zu beschreiben. Ein von der nationalen Zertifizierungsbehörde für diese Stufe zugelassenes Verfahren muß angewendet werden, welches die Authentizität des ausgelieferten EVG garantiert. Bei der Generierung des EVG müssen alle Generierungsoptionen und/oder Änderungen so protokolliert werden, daß es später möglich ist, exakt zu rekonstruieren wie und wann der EVG generiert wurde.

Anforderungen an Nachweise

E4.33 Die vorgelegten Informationen müssen beschreiben, wie die genannten Verfahren die Sicherheit aufrechterhalten.

Aufgaben des Evaluators

E4.34 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die korrekte Anwendung der Auslieferungsverfahren ist zu überprüfen. Es ist nach Fehlern in den Verfahren zur Systemgenerierung zu suchen.

Aspekt 2 - Anlauf und Betrieb

Anforderungen an Prozeduren und Standards

E4.35 Die Prozeduren für einen sicheren Anlauf und Betrieb müssen beschrieben werden. Wenn irgendwelche sicherheitsspezifischen Funktionen während des Anlaufs, des normalen Betriebes oder der Wartung ausgeschaltet oder modifiziert werden können, so muß dies beschrieben werden. **Verfahren müssen vorhanden sein, die den EVG nach einem Systemausfall oder nach einem Hard- oder Softwarefehler in einen sicheren Zustand zurückversetzen können.** Wenn der EVG sicherheitsspezifische Hardware-Komponenten enthält, dann müssen hierfür Diagnoseeinrichtungen vorhanden sein, die durch den Administrator, den Benutzer oder selbsttätig in der Einsatzumgebung aktiviert werden können.

Anforderungen an Nachweise

E4.36 Die vorgelegten Informationen müssen beschreiben, wie die Prozeduren die Sicherheit aufrechterhalten. Der Antragsteller muß Beispiele von Ergebnissen aller Diagnoseprozeduren der in Hardware implementierten sicherheitsspezifischen Komponenten zur Verfügung stellen. Der Antragsteller muß Beispiele aller Protokollaufzeichnungen vorlegen, die während des Anlaufs und des Betriebes erstellt werden.

Aufgaben des Evaluators

E4.37 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die beispielhaften Nachweise für den Anlauf und den Betrieb sind zu überprüfen. Es ist nach Fehlern in den Prozeduren zu suchen.

Stufe E5

Konstruktion - Der Entwicklungsprozeß

E5.1 Der Antragsteller muß den EVG und die folgende Dokumentation bereitstellen:

- Die Sicherheitsvorgaben für den EVG
- Definition eines zugrundeliegenden formal spezifizierten Sicherheitsmodells oder Verweis auf ein solches
- informelle Interpretation des zugrundeliegenden Modells bezüglich der Sicherheitsvorgaben
- semiformale Beschreibung der Architektur des EVG
- semiformale Beschreibung des Feinentwurfs
- Testdokumentation
- Bibliothek der Testprogramme und -werkzeuge, die für den Test des EVG benutzt wurden
- Quellcode bzw. Hardware-Konstruktionszeichnungen für alle sicherheitsspezifischen und sicherheitsrelevanten Komponenten
- informelle Zuordnungsbeschreibung, die den Bezug zwischen Quellcode bzw. Hardware-Konstruktionszeichnungen und dem Feinentwurf darstellt

Phase 1 - Anforderungen

Anforderungen an Inhalt und Form

E5.2 Die Sicherheitsvorgaben muß die sicherheitsspezifischen Funktionen **erklären**, die vom EVG zur Verfügung gestellt werden. Im Falle eines Systems muß die Sicherheitsvorgaben zusätzlich eine System-Sicherheitspolitik (SSP) enthalten, die die Sicherheitsziele und Bedrohungen des Systems identifiziert. Für ein Produkt muß die Sicherheitsvorgaben zusätzliche Aussagen enthalten, die die Art des Produkteinsatzes, die vorgesehene Einsatzumgebung und die für diese Einsatzumgebung angenommenen Bedrohungen identifizieren. Ein formales Sicherheitsmodell oder ein Verweis auf ein solches muß zur Verfügung gestellt werden. Darin ist die zugrundeliegende Sicherheitspolitik zu definieren, die vom EVG durchgesetzt werden muß. Eine informelle Interpretation dieses Modells in Bezug zu den Sicherheitsvorgaben muß zur Verfügung gestellt werden. Die in den Sicherheitsvorgaben aufgeführten sicherheitsspezifischen Funktionen müssen sowohl in informeller als auch in semiformaler Notation (siehe Kapitel 2) spezifiziert werden.

Anforderungen an Nachweise

E5.3 Im Falle eines Systems müssen die Sicherheitsvorgaben **erklären**, auf welche Weise die vorgeschlagene Funktionalität die Sicherheitsziele erfüllt und wie sie den definierten Bedrohungen angemessen entgegenwirkt. Im Fall eines Produktes müssen die Sicherheitsvorgaben **erklären**, warum die Funktionalität für diese Art des Einsatzes zweckmäßig ist und wie sie den angenommenen Bedrohungen entgegenwirkt. Die informelle Interpretation des formalen Sicherheitsmodells muß **erklären**, auf welche Weise seine zugrundeliegende Sicherheitspolitik durch die Sicherheitsvorgaben erfüllt wird.

Aufgaben des Evaluators

E5.4 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist zu überprüfen, ob es Inkonsistenzen innerhalb der Sicherheitsvorgaben gibt. Es ist zu überprüfen, ob es Sicherheitsmaßnahmen in den Sicherheitsvorgaben gibt, die zu Konflikten mit der dem Sicherheitsmodell zugrundeliegenden Sicherheitspolitik führen.

Phase 2 - Architekturentwurf

Anforderungen an Inhalt und Form

E5.5 Eine semiformale Notation muß verwendet werden, um einen semiformalen Architekturentwurf zu erstellen. Diese Beschreibung muß die grundsätzliche Struktur sowie alle externen Schnittstellen des EVG **erklären**. Sie muß die Hard- und Firmware **erklären**, die der EVG benötigt, und die Funktionalität der unterstützenden Schutzmechanismen angeben, die in dieser Hard- oder Firmware implementiert sind. Sie muß die Aufteilung des EVG in sicherheitsspezifische und andere Komponenten **erklären. Sie muß die Beziehungen der sicherheitsspezifischen Komponenten zueinander erklären.**

Anforderungen an Nachweise

E5.6 Die Beschreibung der Architektur muß **erklären**, wie die sicherheitsspezifischen Funktionen der Sicherheitsvorgaben zur Verfügung gestellt werden. Sie muß **erklären**, wie die Trennung in sicherheitsspezifische und andere Komponenten erreicht wird. Sie muß **erklären**, auf welche Weise die gewählte Struktur die größtmögliche Unabhängigkeit der sicherheitsspezifischen Komponenten gewährleistet. **Sie muß erklären, warum die Beziehungen zwischen den sicherheitsspezifischen Komponenten notwendig sind.**

Aufgaben des Evaluators

E5.7 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist zu überprüfen, ob die Trennung von sicherheitsspezifischen und anderen Komponenten wirksam ist.

Phase 3 - Feinentwurf

Anforderungen an Inhalt und Form

E5.8 Eine semiformale Notation muß verwendet werden, um einen semiformalen Feinentwurf zu erstellen. Der Feinentwurf muß alle Basiskomponenten spezifizieren. Er muß durch alle Ebenen der Entwurfshierarchie die Realisierung aller sicherheitsspezifischen und aller sicherheitsrelevanten Funktionen **erklären**. Er muß die Aufteilung des EVG in sicherheitsspezifische, sicherheitsrelevante und in andere Komponenten **erklären**. Er muß in klar definierte, weitgehend voneinander unabhängige Basiskomponenten aufgegliedert sein, die das Testen erleichtern und die Möglichkeiten zu einer Verletzung der Sicherheit minimieren. **Er muß weitgehend die Konzepte der hierarchischen Dekomposition, der Abstraktion und der Datenabschottung anwenden.** Er muß alle Sicherheitsmechanismen identifizieren. Er muß die sicherheitsspezifischen Funktionen auf Mechanismen **und Funktionseinheiten** abbilden. **Sicherheitsspezifische und sicherheitsrelevante Komponenten dürfen keine unnötige Funktionalität enthalten.** Alle Schnittstellen der sicherheitsspezifischen und der sicherheitsrelevanten Komponenten müssen mit ihrem Zweck, ihren Parametern und **ihren Auswirkungen** dokumentiert werden. **Der Zweck aller Variablen, die von mehr als einer Funktionseinheit benutzt werden, muß erklärt werden.** Spezifikationen/Definitionen für die Mechanismen müssen zur Verfügung gestellt werden. Diese Spezifikationen müssen für die Analyse der Beziehungen zwischen den verwendeten Mechanismen geeignet sein. Für Komponenten, die weder sicherheitsspezifisch noch sicherheitsrelevant sind, müssen keine Spezifikationen zur Verfügung gestellt werden. Wo mehr als eine Spezifikationsebene vorliegt, muß eine klare und hierarchische Beziehung zwischen den Ebenen bestehen.

Anforderung an Nachweise

E5.9 Die Feinentwurf muß **erklären**, auf welche Weise die Sicherheitsmechanismen die sicherheitsspezifischen Funktionen, die in den Sicherheitsvorgaben spezifiziert sind, realisieren. **Er muß erklären, warum die verbleibende Funktionalität aus den sicherheitsspezifischen und den sicherheitsrelevanten Komponenten nicht ausgeklammert werden kann.** Er muß **erklären**, warum Komponenten, für die keine Entwurfsunterlagen zur Verfügung gestellt werden, weder sicherheitsspezifisch noch sicherheitsrelevant sein können.

Aufgaben des Evaluators

E5.10 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Phase 4 - Implementierung

Anforderungen an Inhalt und Form

E5.11 **Der Quellcode und die Hardware-Konstruktionszeichnungen müssen vollständig in kleine, verständliche und getrennte Teile aufgegliedert sein.** Die Zuordnungsbeschreibung muß die Übereinstimmung zwischen Quellcode bzw. Hardware-Konstruktionszeichnungen und den **Funktionseinheiten** des Feinentwurfs **erklären**. Die Testdokumentation muß Testpläne, Testziele, Testverfahren und Testergebnisse enthalten und eine Begründung, warum die gewählte Testabdeckung ausreicht. Die Bibliothek von Testprogrammen muß Testprogramme und -werkzeuge enthalten, mit denen alle Tests, die in der Testdokumentation beschrieben sind, wiederholt werden können.

Anforderungen an Nachweise

E5.12 Die Testdokumentation muß die Übereinstimmung zwischen den Tests und den in den Sicherheitsvorgaben definierten sicherheitsspezifischen Funktionen **erklären**. Sie muß die Übereinstimmung zwischen den Tests und den sicherheitsspezifischen und sicherheitsrelevanten Funktionen **erklären**, die im Feinentwurf definiert sind. Sie muß die Übereinstimmung zwischen den Tests und den Sicherheitsmechanismen **erklären**, wie sie im Quellcode bzw. in den Hardware-Konstruktionszeichnungen dargestellt sind. Nachweise über Wiederholungstests nach der Entdeckung und Korrektur sicherheitsrelevanter Fehler sind zwingend, um zu zeigen, daß die Fehler behoben wurden und daß keine neuen Fehler eingefügt wurden.

Aufgaben des Evaluators

E5.13 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die Bibliothek der Testprogramme ist für eine stichprobenweise Überprüfung der Testergebnisse heranzuziehen. Es ist zu überprüfen, ob die Tests alle sicherheitsspezifischen Funktionen, die in den Sicherheitsvorgaben angegeben sind, umfassen. Es ist zu überprüfen, ob die Tests alle im Feinentwurf identifizierten sicherheitsspezifischen und sicherheitsrelevanten Funktionen sowie alle im Quellcode bzw. in den Hardware-Konstruktionszeichnungen identifizierbaren Sicherheitsmechanismen umfassen. Alle Wiederholungstests, die auf die Fehlerkorrektur erfolgten, sind zu überprüfen. Zusätzlich sind Tests zur Fehlersuche durchzuführen.

Konstruktion - Die Entwicklungsumgebung

E5.14 Der Antragsteller muß die folgende Dokumentation bereitstellen:

- Konfigurationsliste, die die Version des EVG für die Evaluation identifiziert
- Informationen über das Konfigurationskontrollsystem und seine Werkzeuge

- Protokollinformationen über Änderungen aller **Objekte** des EVG, die der Konfigurationskontrolle unterliegen
- Informationen über das Abnahmeverfahren
- **Informationen über das Integrationsverfahren**
- Informationen über die Sicherheit der Entwicklungsumgebung
- Beschreibung aller benutzten Implementierungssprachen und Compiler
- **Quellcode aller benutzten Laufzeitbibliotheken**

Aspekt 1 - Konfigurationskontrolle

Anforderungen an Inhalt und Form

E5.15 Der Entwicklungsvorgang muß durch ein, durch Werkzeuge unterstütztes, Konfigurationskontrollsystem und Abnahmeverfahren unterstützt werden. **Die Werkzeuge zur Konfigurationskontrolle müssen sicherstellen, daß die Person, die für die Aufnahme eines Objektes in die Konfigurationskontrolle verantwortlich ist, nicht für dessen Entwurf oder Entwicklung zuständig war.** Die vorgelegte Konfigurationsliste muß alle Basiskomponenten auflisten, aus denen der EVG besteht. Der EVG, seine Basiskomponenten und alle zur Verfügung gestellten Dokumente, einschließlich der Handbücher und des Quellcodes bzw. der Hardware-Konstruktionszeichnungen, müssen eine eindeutige Identifikation besitzen. Die Verwendung dieser Identifikation bei Verweisen wird zwingend vorgeschrieben. Das Konfigurationskontrollsystem muß sicherstellen, daß der in Evaluation befindliche EVG mit der zur Verfügung gestellten Dokumentation übereinstimmt und daß nur autorisierte Änderungen durch autorisierte Personen möglich sind. **Alle Objekte, die während des Entwicklungsprozesses entstehen und die durch das Abnahmeverfahren laufen, müssen der Konfigurationskontrolle unterliegen. Alle sicherheitsspezifischen und alle sicherheitsrelevanten Objekte, die der Konfigurationskontrolle unterliegen, müssen als solche gekennzeichnet sein.** Die Werkzeuge des Konfigurationskontrollsystems müssen in der Lage sein, Änderungen zwischen unterschiedlichen Versionen von Objekten, die der Konfigurationskontrolle unterworfen sind, zu überwachen und zu protokollieren. **Alle Änderungen dieser Objekte müssen protokolliert werden, mit Angabe desjenigen, der die Änderung durchgeführt hat sowie mit Datum und Uhrzeit. Die Werkzeuge zur Konfigurationskontrolle müssen in der Lage sein, die Erzeugung und die Behandlung von variablen Beziehungen zwischen Objekten, die der Konfigurationskontrolle unterliegen, zu unterstützen. Im Falle der Änderung an irgendeinem dieser Objekte müssen die Werkzeuge in der Lage sein, alle anderen Objekte unter Konfigurationskontrolle, die von dieser Änderung betroffen sind, aufzuzeigen, zusammen mit einer Angabe, ob es sich dabei um sicherheitsspezifische oder sicherheitsrelevante Objekte handelt.**

Anforderungen an Nachweise

E5.16 Die Informationen über das Konfigurationskontrollsystem **und das Integrationsverfahren** müssen **erklären**, wie **sie** in der Praxis benutzt **werden** und wie **sie** im Entwicklungsprozeß zusammen mit den Qualitätsmanagementverfahren des Herstellers angewendet **werden**. **Die Informationen über das Konfigurationskontrollsystem müssen erklären, wie die Werkzeuge sicherstellen, daß eine Person, die für die Abnahme eines Objektes verantwortlich ist, nicht an dessen Entwurf oder Entwicklung beteiligt war. Beispiele der Protokolle des Konfigurationskontrollsystems müssen zur Verfügung gestellt werden.**

Aufgaben des Evaluators

E5.17 Es ist zu überprüfen, ob die dokumentierten Verfahren angewendet werden. Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. **Die Protokoll-Beispiele sind zu überprüfen.** Ausgewählte Teile des EVG sind unter Verwendung der Werkzeuge des Entwicklers neu zu montieren; die Ergebnisse sind mit dem vorliegenden EVG zu vergleichen.

Aspekt 2 - Programmiersprachen und Compiler

Anforderungen an Inhalt und Form

E5.18 Alle Programmiersprachen, die für die Implementierung benutzt werden, müssen klar definiert sein, wie z.B. in einem ISO-Standard. Alle implementierungsabhängigen Optionen der Programmiersprache müssen dokumentiert sein. Für alle benutzten Compiler müssen die gewählten Implementierungsoptionen dokumentiert werden. **Der Quellcode aller Laufzeitbibliotheken muß zur Verfügung gestellt werden.**

Anforderungen an Nachweise

E5.19 Die Definition der jeweiligen Programmiersprache muß die Bedeutung aller Anweisungen, die im Quellcode benutzt werden, eindeutig festlegen.

Aufgaben des Evaluators

E5.20 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Aspekt 3 - Sicherheit beim Entwickler

Anforderungen an Inhalt und Form

E5.21 Das Dokument über die Sicherheit der Entwicklungsumgebung muß die geplanten Schutzmaßnahmen bzgl. der Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumente **erklären**. Materielle, organisatorische, personelle und andere Sicherheitsmaßnahmen, die durch den Entwickler eingesetzt werden, müssen **erklärt** werden.

Anforderungen an Nachweise

E5.22 Die Information über die Sicherheit der Entwicklungsumgebung muß **erklären**, wie die Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumentation gewährleistet werden.

Aufgaben des Evaluators

E5.23 Es ist zu überprüfen, ob die dokumentierten Verfahren angewendet werden. Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist nach Fehlern in den Verfahren zu suchen.

Betrieb - Die Betriebsdokumentation

E5.24 Der Antragsteller muß die folgende Dokumentation bereitstellen:

- Benutzerdokumentation
- Systemverwalter-Dokumentation

Aspekt 1 - Benutzerdokumentation

Anforderungen an Inhalt und Form

E5.25 Die Benutzerdokumentation muß die sicherheitsspezifischen Funktionen, die für den Endnutzer von Bedeutung sind, **erklären**. Daneben muß sie auch Richtlinien für ihre sichere Anwendung enthalten. Die Benutzerdokumentation, zu welcher beispielsweise Referenz-Manuale, Benutzeranleitungen etc. gehören, muß strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.

Anforderungen an Nachweise

E5.26 Die Benutzerdokumentation muß **erklären**, wie ein Endnutzer den EVG in einer sicheren Art und Weise nutzt.

Aufgaben des Evaluators

E5.27 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Aspekt 2 - Systemverwalter-Dokumentation

Anforderungen an Inhalt und Form

E5.28 Die Systemverwalter-Dokumentation muß die sicherheitsspezifischen Funktionen **erklären**, die für den Systemverwalter von Bedeutung sind. Sie muß zwei Funktionsarten unterscheiden: solche, mit denen der Systemverwalter die Sicherheitsparameter kontrollieren kann, und solche, mit denen er lediglich Informationen abfragen kann. Wenn ein Systemverwalter notwendig ist, muß sie alle Sicherheitsparameter **erklären**, die er kontrollieren kann. Sie muß jeden Typ eines sicherheitsrelevanten Ereignisses **erklären**, der für die Systemverwaltungsfunktionen von Bedeutung ist. Sie muß Details zu den Verfahren, die für die Sicherheitsadministration relevant sind, in einer Form **erklären**, die für die Handhabung ausreichend ist. Sie muß Richtlinien zu der konsistenten und wirksamen Nutzung der Sicherheitseigenschaften des EVG enthalten und **erklären**, wie solche Eigenschaften zusammenwirken. Sie muß die Anweisungen **erklären**, wie das System/Produkt installiert wird und wie es, wenn erforderlich, konfiguriert wird. Die Systemverwalter-Dokumentation, z.B. Referenz-Manuale, Systemverwalter-Anleitungen etc., muß strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.

Anforderungen an Nachweise

E5.29 Die Systemverwalter-Dokumentation muß **erklären**, wie der EVG sicher verwaltet wird.

Aufgaben des Evaluators

E5.30 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Betrieb - Die Betriebsumgebung

E5.31 Der Antragsteller hat die folgende Dokumentation bereitzustellen:

- Auslieferungs- und Konfigurations-Dokumentation
- Anlauf- und Betriebs-Dokumentation

Aspekt 1 - Auslieferung und Konfiguration

Anforderungen an Prozeduren und Standards

E5.32 Wenn unterschiedliche Konfigurationen möglich sind, muß die Auswirkung der einzelnen Konfigurationen auf die Sicherheit **erklärt** werden. Die Verfahren der Auslieferung und Systemgenerierung sind zu **erklären**. Ein von der nationalen Zertifizierungsbehörde für diese Stufe zugelassenes Verfahren muß angewendet werden, welches die Authentizität des ausgelieferten EVG garantiert. Bei der Generierung des EVG müssen alle Generierungsoptionen und/oder Änderungen so protokolliert werden, daß es später möglich ist, exakt zu rekonstruieren wie und wann der EVG generiert wurde.

Anforderungen an Nachweise

E5.33 Die vorgelegten Informationen müssen **erklären**, wie die genannten Verfahren die Sicherheit aufrechterhalten.

Aufgaben des Evaluators

E5.34 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die korrekte Anwendung der Auslieferungsverfahren ist zu überprüfen. Es ist nach Fehlern in den Verfahren zur Systemgenerierung zu suchen.

Aspekt 2 - Anlauf und Betrieb

Anforderungen an Prozeduren und Standards

E5.35 Die Prozeduren für einen sicheren Anlauf und Betrieb müssen **erklärt** werden. Wenn irgendwelche sicherheitsspezifischen Funktionen während des Anlaufs, des normalen Betriebes oder der Wartung ausgeschaltet oder modifiziert werden können, so muß dies **erklärt** werden. Verfahren müssen vorhanden sein, die den EVG nach einem Systemausfall oder nach einem Hard- oder Softwarefehler in einen sicheren Zustand zurückversetzen können. Wenn der EVG sicherheitsspezifische Hardware-Komponenten enthält, dann müssen hierfür Diagnoseeinrichtungen vorhanden sein, die durch den

Administrator, den Benutzer oder selbsttätig in der Einsatzumgebung aktiviert werden können.

Anforderungen an Nachweise

E5.36 Die vorgelegten Informationen müssen **erklären**, wie die Prozeduren die Sicherheit aufrechterhalten. Der Antragsteller muß Beispiele von Ergebnissen aller Diagnoseprozeduren der in Hardware implementierten sicherheitsspezifischen Komponenten zur Verfügung stellen. Der Antragsteller muß Beispiele aller Protokollaufzeichnungen vorlegen, die während des Anlaufs und des Betriebes erstellt werden.

Aufgaben des Evaluators

E5.37 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die beispielhaften Nachweise für den Anlauf und den Betrieb sind zu überprüfen. Es ist nach Fehlern in den Prozeduren zu suchen.

Stufe E6

Konstruktion - Der Entwicklungsprozeß

E6.1 Der Antragsteller muß den EVG und die folgende Dokumentation bereitstellen:

- Die Sicherheitsvorgaben für den EVG
- Definition eines zugrundeliegenden formal spezifizierten Sicherheitsmodells oder Verweis auf ein solches
- informelle Interpretation des zugrundeliegenden Modells bezüglich der Sicherheitsvorgaben
- **formale** Beschreibung der Architektur des EVG
- semiformale Beschreibung des Feinentwurfs
- Testdokumentation
- Bibliothek der Testprogramme und -werkzeuge, die für den Test des EVG benutzt wurden, **einschließlich der Werkzeuge, welche dazu verwendet werden können, Inkonsistenzen zwischen Quellcode und ausführbarem Code zu entdecken, sofern es sicherheitsspezifische oder sicherheitsrelevante Quellcodekomponenten gibt (z.B. Disassembler und/oder Debugger)**
- Quellcode bzw. Hardware-Konstruktionszeichnungen für alle sicherheitsspezifischen und sicherheitsrelevanten Komponenten
- informelle Zuordnungsbeschreibung, die den Bezug zwischen Quellcode bzw. Hardware-Konstruktionszeichnungen, dem Feinentwurf **und der formalen Spezifikation der sicherheitsspezifischen Funktionen** darstellt

Phase 1 - Anforderungen

Anforderungen an Inhalt und Form

E6.2 Die Sicherheitsvorgaben muß die sicherheitsspezifischen Funktionen erklären, die vom EVG zur Verfügung gestellt werden. Im Falle eines Systems müssen die Sicherheitsvorgaben zusätzlich eine System-Sicherheitspolitik (SSP) enthalten, die die Sicherheitsziele und Bedrohungen des Systems identifiziert. Für ein Produkt müssen die Sicherheitsvorgaben zusätzliche Aussagen enthalten, die die Art des Produkteinsatzes, die vorgesehene Einsatzumgebung und die für diese Einsatzumgebung angenommenen Bedrohungen identifizieren. Ein formales Sicherheitsmodell oder ein Verweis auf ein solches muß zur Verfügung gestellt werden. Darin ist die zugrundeliegende Sicherheitspolitik zu definieren, die vom EVG durchgesetzt werden muß. Eine informelle

Interpretation dieses Modells in Bezug zu den Sicherheitsvorgaben muß zur Verfügung gestellt werden. Die in den Sicherheitsvorgaben aufgeführten sicherheitsspezifischen Funktionen müssen sowohl in informeller als auch in **formaler** Notation (siehe Kapitel 2) spezifiziert werden.

Anforderungen an Nachweise

E6.3 Im Falle eines Systems müssen die Sicherheitsvorgaben erklären, auf welche Weise die vorgeschlagene Funktionalität die Sicherheitsziele erfüllt und wie sie den definierten Bedrohungen angemessen entgegenwirkt. Im Falle eines Produktes müssen die Sicherheitsvorgaben erklären, warum die Funktionalität für diese Art des Einsatzes zweckmäßig ist und wie sie den angenommenen Bedrohungen entgegenwirkt. Die informelle Interpretation des formalen Sicherheitsmodells muß erklären, auf welche Weise seine zugrundeliegende Sicherheitspolitik durch die Sicherheitsvorgaben erfüllt wird.

Aufgaben des Evaluators

E6.4 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist zu überprüfen, ob es Inkonsistenzen innerhalb der Sicherheitsvorgaben gibt. Es ist zu überprüfen, ob es Sicherheitsmaßnahmen in den Sicherheitsvorgaben gibt, die zu Konflikten mit der dem Sicherheitsmodell zugrundeliegenden Sicherheitspolitik führen.

Phase 2 - Architekturentwurf

Anforderungen an Inhalt und Form

E6.5 Eine **formale** Notation muß verwendet werden, um einen **formalen** Architekturentwurf zu erstellen. Diese Beschreibung muß die grundsätzliche Struktur sowie alle externen Schnittstellen des EVG erklären. Sie muß die Hard- und Firmware erklären, die der EVG benötigt, und die Funktionalität der unterstützenden Schutzmechanismen angeben, die in dieser Hard- oder Firmware implementiert sind. Sie muß die Aufteilung des EVG in sicherheitsspezifische und andere Komponenten erklären. Sie muß die Beziehungen der sicherheitsspezifischen Komponenten zueinander erklären.

Anforderungen an Nachweise

E6.6 Die Beschreibung der Architektur muß erklären, wie die sicherheitsspezifischen Funktionen der Sicherheitsvorgaben zur Verfügung gestellt werden. Sie muß erklären, wie die Trennung in sicherheitsspezifische und andere Komponenten erreicht wird. Sie muß erklären, auf welche Weise die gewählte Struktur die größtmögliche Unabhängigkeit der sicherheitsspezifischen Komponenten gewährleistet. **Sie muß erklären, warum die Beziehungen zwischen den sicherheitsspezifischen Komponenten notwendig sind. Sie muß durch Anwendung einer Mischung von formaler und**

informeller Technik erklären, wie sie mit dem formalen Sicherheitsmodell übereinstimmt.

Aufgaben des Evaluators

E6.7 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist zu überprüfen, ob die Trennung von sicherheitsspezifischen und anderen Komponenten wirksam ist. **Es ist zu überprüfen, ob die formalen Argumente gültig sind.**

Phase 3 - Feinentwurf

Anforderungen an Inhalt und Form

E6.8 Eine semiformale Notation muß verwendet werden, um einen semiformalen Feinentwurf zu erstellen. Der Feinentwurf muß alle Basiskomponenten spezifizieren. Er muß durch alle Ebenen der Entwurfshierarchie die Realisierung aller sicherheitsspezifischen und aller sicherheitsrelevanten Funktionen erklären. Er muß die Aufteilung des EVG in sicherheitsspezifische, sicherheitsrelevante und in andere Komponenten erklären. Er muß in klar definierte, weitgehend voneinander unabhängige Basiskomponenten aufgegliedert sein, die das Testen erleichtern und die Möglichkeiten zu einer Verletzung der Sicherheit minimieren. Er muß weitgehend die Konzepte der hierarchischen Dekomposition, der Abstraktion und der Datenabschottung anwenden. Er muß alle Sicherheitsmechanismen identifizieren. Er muß die sicherheitsspezifischen Funktionen auf Mechanismen und Funktionseinheiten abbilden. Sicherheitsspezifische und sicherheitsrelevante Komponenten dürfen keine unnötige Funktionalität enthalten. Alle Schnittstellen der sicherheitsspezifischen und der sicherheitsrelevanten Komponenten müssen mit ihrem Zweck, ihren Parametern und ihren Auswirkungen dokumentiert werden. Der Zweck aller Variablen, die von mehr als einer Funktionseinheit benutzt werden, muß erklärt werden. Spezifikationen/Definitionen für die Mechanismen müssen zur Verfügung gestellt werden. Diese Spezifikationen müssen für die Analyse der Beziehungen zwischen den verwendeten Mechanismen geeignet sein. Für Komponenten, die weder sicherheitsspezifisch noch sicherheitsrelevant sind, müssen keine Spezifikationen zur Verfügung gestellt werden. Wo mehr als eine Spezifikationsebene vorliegt, muß eine klare und hierarchische Beziehung zwischen den Ebenen bestehen.

Anforderung an Nachweise

E6.9 Der Feinentwurf muß erklären, auf welche Weise die Sicherheitsmechanismen die sicherheitsspezifischen Funktionen, die in den Sicherheitsvorgaben spezifiziert sind, realisieren. Er muß erklären, warum die verbleibende Funktionalität aus den sicherheitsspezifischen und den sicherheitsrelevanten Komponenten nicht ausgeklammert werden kann. Er muß erklären, warum Komponenten, für die keine Entwurfsunterlagen zur Verfügung gestellt werden, weder sicherheitsspezifisch noch sicherheitsrelevant sein können.

Aufgaben des Evaluators

E6.10 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Phase 4 - Implementierung

Anforderungen an Inhalt und Form

E6.11 Der Quellcode und die Hardware-Konstruktionszeichnungen müssen vollständig in kleine, verständliche und getrennte Teile aufgegliedert sein. Die Zuordnungsbeschreibung muß die Übereinstimmung zwischen Quellcode bzw. Hardware-Konstruktionszeichnungen und den Funktionseinheiten des Feinentwurfs erklären. **Sie muß die Übereinstimmung zwischen den Sicherheitsmechanismen, wie im Quellcode bzw. in den Hardware-Konstruktionszeichnungen dargestellt, und der formalen Spezifikation der sicherheitsspezifischen Funktionen in den Sicherheitsvorgaben erklären.** Die Testdokumentation muß Testpläne, Testziele, Testverfahren und Testergebnisse enthalten und eine Begründung, warum die gewählte Testabdeckung ausreicht. Die Bibliothek von Testprogrammen muß Testprogramme und -werkzeuge enthalten, mit denen alle Tests, die in der Testdokumentation beschrieben sind, wiederholt werden können.

Anforderungen an Nachweise

E6.12 Die Testdokumentation muß die Übereinstimmung zwischen den Tests und der **formalen Spezifikation der** in den Sicherheitsvorgaben definierten sicherheitsspezifischen Funktionen erklären. Sie muß die Übereinstimmung zwischen den Tests und den sicherheitsspezifischen und sicherheitsrelevanten Funktionen erklären, die im Feinentwurf definiert sind. Sie muß die Übereinstimmung zwischen den Tests und den Sicherheitsmechanismen erklären, wie sie im Quellcode bzw. in den Hardware-Konstruktionszeichnungen dargestellt sind. Nachweise über Wiederholungstests nach der Entdeckung und Korrektur sicherheitsrelevanter Fehler sind zwingend, um zu zeigen, daß die Fehler behoben wurden und daß keine neuen Fehler eingefügt wurden.

Aufgaben des Evaluators

E6.13 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die Bibliothek der Testprogramme ist für eine stichprobenweise Überprüfung der Testergebnisse heranzuziehen. Es ist zu überprüfen, ob die Tests alle sicherheitsspezifischen Funktionen, die in den Sicherheitsvorgaben angegeben sind, umfassen. Es ist zu überprüfen, ob die Tests alle im Feinentwurf identifizierten sicherheitsspezifischen und sicherheitsrelevanten Funktionen sowie alle im Quellcode bzw. in den Hardware-Konstruktionszeichnungen identifizierbaren Sicherheitsmechanismen umfassen. Alle Wiederholungstests, die auf die Fehlerkorrektur erfolgten, sind zu überprüfen. Zusätzlich sind Tests zur Fehlersuche durchzuführen. **Alle mutmaßlichen Inkonsistenzen zwischen Quellcode und ausführbarem Code, die**

während der Tests mit den vom Antragsteller gelieferten Werkzeugen gefunden wurden, sind zu untersuchen.

Konstruktion - Die Entwicklungsumgebung

E6.14 Der Antragsteller muß die folgende Dokumentation bereitstellen:

- Konfigurationsliste, die die Version des EVG für die Evaluation identifiziert
- Informationen über das Konfigurationskontrollsystem und seine Werkzeuge
- Protokollinformationen über Änderungen aller Objekte des EVG, die der Konfigurationskontrolle unterliegen
- Informationen über das Abnahmeverfahren
- Informationen über das Integrationsverfahren
- Informationen über die Sicherheit der Entwicklungsumgebung
- Beschreibung aller benutzten Implementierungssprachen und Compiler
- Quellcode aller benutzten Laufzeitbibliotheken

Aspekt 1 - Konfigurationskontrolle

Anforderungen an Inhalt und Form

E6.15 Der Entwicklungsvorgang muß durch ein, durch Werkzeuge unterstütztes, Konfigurationskontrollsystem und Abnahmeverfahren unterstützt werden. Die Werkzeuge zur Konfigurationskontrolle müssen sicherstellen, daß die Person, die für die Aufnahme eines Objektes in die Konfigurationskontrolle verantwortlich ist, nicht für dessen Entwurf oder Entwicklung zuständig war. Die vorgelegte Konfigurationsliste muß alle Basiskomponenten auflisten, aus denen der EVG besteht. Der EVG, seine Basiskomponenten und alle zur Verfügung gestellten Dokumente, einschließlich der Handbücher und des Quellcodes bzw. der Hardware-Konstruktionszeichnungen, müssen eine eindeutige Identifikation besitzen. Die Verwendung dieser Identifikation bei Verweisen wird zwingend vorgeschrieben. Das Konfigurationskontrollsystem muß sicherstellen, daß der in Evaluation befindliche EVG mit der zur Verfügung gestellten Dokumentation übereinstimmt und daß nur autorisierte Änderungen durch autorisierte Personen möglich sind. **Alle Werkzeuge, die im Entwicklungsprozeß benutzt werden, müssen der Konfigurationskontrolle unterliegen.** Alle Objekte, die während des Entwicklungsprozesses entstehen und die durch das Abnahmeverfahren laufen, müssen der Konfigurationskontrolle unterliegen. Alle sicherheitsspezifischen und alle sicherheitsrelevanten Objekte, die der Konfigurationskontrolle unterliegen, müssen als solche gekennzeichnet sein. Die Werkzeuge des Konfigurationskontrollsystems müssen in der Lage sein, Änderungen zwischen unterschiedlichen Versionen von Objekten, die

der Konfigurationskontrolle unterworfen sind, zu überwachen und zu protokollieren. Alle Änderungen dieser Objekte müssen protokolliert werden, mit Angabe desjenigen, der die Änderung durchgeführt hat sowie mit Datum und Uhrzeit. Die Werkzeuge zur Konfigurationskontrolle müssen in der Lage sein, die Erzeugung und die Behandlung von variablen Beziehungen zwischen Objekten, die der Konfigurationskontrolle unterliegen, zu unterstützen. Im Falle der Änderung an irgendeinem dieser Objekte müssen die Werkzeuge in der Lage sein, alle anderen Objekte unter Konfigurationskontrolle, die von dieser Änderung betroffen sind, aufzuzeigen, zusammen mit einer Angabe, ob es sich dabei um sicherheitsspezifische oder sicherheitsrelevante Objekte handelt.

Anforderungen an Nachweise

E6.16 Die Informationen über das Konfigurationskontrollsystem und das Integrationsverfahren müssen erklären, wie sie in der Praxis benutzt werden und wie sie im Entwicklungsprozeß zusammen mit den Qualitätsmanagementverfahren des Herstellers angewendet werden. Die Informationen über das Konfigurationskontrollsystem müssen erklären, wie die Werkzeuge sicherstellen, daß eine Person, die für die Abnahme eines Objektes verantwortlich ist, nicht an dessen Entwurf oder Entwicklung beteiligt war. Beispiele der Protokolle des Konfigurationskontrollsystems müssen zur Verfügung gestellt werden.

Aufgaben des Evaluators

E6.17 Es ist zu überprüfen, ob die dokumentierten Verfahren angewendet werden. Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die Protokoll-Beispiele sind zu überprüfen. Ausgewählte Teile des EVG sind unter Verwendung der Werkzeuge des Entwicklers neu zu montieren; die Ergebnisse sind mit dem vorliegenden EVG zu vergleichen.

Aspekt 2 - Programmiersprachen und Compiler

Anforderungen an Inhalt und Form

E6.18 Alle Programmiersprachen, die für die Implementierung benutzt werden, müssen klar definiert sein, wie z.B. in einem ISO-Standard. Alle implementierungsabhängigen Optionen der Programmiersprache müssen dokumentiert sein. Für alle benutzten Compiler müssen die gewählten Implementierungsoptionen dokumentiert werden. Der Quellcode aller Laufzeitbibliotheken muß zur Verfügung gestellt werden.

Anforderungen an Nachweise

E6.19 Die Definition der jeweiligen Programmiersprache muß die Bedeutung aller Anweisungen, die im Quellcode benutzt werden, eindeutig festlegen.

Aufgaben des Evaluators

E6.20 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Aspekt 3 - Sicherheit beim Entwickler

Anforderungen an Inhalt und Form

E6.21 Das Dokument über die Sicherheit der Entwicklungsumgebung muß die geplanten Schutzmaßnahmen bzgl. der Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumente erklären. Materielle, organisatorische, personelle und andere Sicherheitsmaßnahmen, die durch den Entwickler eingesetzt werden, müssen erklärt werden.

Anforderungen an Nachweise

E6.22 Die Information über die Sicherheit der Entwicklungsumgebung muß erklären, wie die Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumentation gewährleistet werden.

Aufgaben des Evaluators

E6.23 Es ist zu überprüfen, ob die dokumentierten Verfahren angewendet werden. Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist nach Fehlern in den Verfahren zu suchen.

Betrieb - Die Betriebsdokumentation

E6.24 Der Antragsteller muß die folgende Dokumentation bereitstellen:

- Benutzerdokumentation
- Systemverwalter-Dokumentation

Aspekt 1 - Benutzerdokumentation

Anforderungen an Inhalt und Form

E6.25 Die Benutzerdokumentation muß die sicherheitsspezifischen Funktionen, die für den Endnutzer von Bedeutung sind, erklären. Daneben muß sie auch Richtlinien für ihre sichere Anwendung enthalten. Die Benutzerdokumentation, zu welcher beispielsweise Referenz-Manuale, Benutzeranleitungen etc. gehören, muß strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.

Anforderungen an Nachweise

E6.26 Die Benutzerdokumentation muß erklären, wie ein Endnutzer den EVG in einer sicheren Art und Weise nutzt.

Aufgaben des Evaluators

E6.27 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Aspekt 2 - Systemverwalter-Dokumentation

Anforderungen an Inhalt und Form

E6.28 Die Systemverwalter-Dokumentation muß die sicherheitsspezifischen Funktionen erklären, die für den Systemverwalter von Bedeutung sind. Sie muß zwei Funktionsarten unterscheiden: solche, mit denen der Systemverwalter die Sicherheitsparameter kontrollieren kann, und solche, mit denen er lediglich Informationen abfragen kann. Wenn ein Systemverwalter notwendig ist, muß sie alle Sicherheitsparameter erklären, die er kontrollieren kann. Sie muß jeden Typ eines sicherheitsrelevanten Ereignisses erklären, der für die Systemverwaltungsfunktionen von Bedeutung ist. Sie muß Details zu den Verfahren, die für die Sicherheitsadministration relevant sind, in einer Form erklären, die für die Handhabung ausreichend ist. Sie muß Richtlinien zu der konsistenten und wirksamen Nutzung der Sicherheitseigenschaften des EVG enthalten und erklären, wie solche Eigenschaften zusammenwirken. Sie muß die Anweisungen erklären, wie das System/Produkt installiert wird und wie es, wenn erforderlich, konfiguriert wird. Die Systemverwalter-Dokumentation, z.B. Referenz-Manuale, Systemverwalter-Anleitungen etc., muß strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.

Anforderungen an Nachweise

E6.29 Die Systemverwalter-Dokumentation muß erklären, wie der EVG sicher verwaltet wird.

Aufgaben des Evaluators

E6.30 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Betrieb - Die Betriebsumgebung

E6.31 Der Antragsteller hat die folgende Dokumentation bereitzustellen:

- Auslieferungs- und Konfigurations-Dokumentation
- Anlauf- und Betriebs-Dokumentation

Aspekt 1 - Auslieferung und Konfiguration

Anforderungen an Prozeduren und Standards

E6.32 Wenn unterschiedliche Konfigurationen möglich sind, **muß sich dies im formalen Architekturentwurf widerspiegeln und** die Auswirkung der einzelnen Konfigurationen auf die Sicherheit muß erklärt werden. Die Verfahren der Auslieferung und Systemgenerierung sind zu erklären. Ein von der nationalen Zertifizierungsbehörde für diese Stufe zugelassenes Verfahren muß angewendet werden, welches die Authentizität des ausgelieferten EVG garantiert. Bei der Generierung des EVG müssen alle Generierungsoptionen und/oder Änderungen so protokolliert werden, daß es später möglich ist, exakt zu rekonstruieren, wie und wann der EVG generiert wurde.

Anforderungen an Nachweise

E6.33 Die vorgelegten Informationen müssen erklären, wie die genannten Verfahren die Sicherheit aufrechterhalten.

Aufgaben des Evaluators

E6.34 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die korrekte Anwendung der Auslieferungsverfahren ist zu überprüfen. Es ist nach Fehlern in den Verfahren zur Systemgenerierung zu suchen.

Aspekt 2 - Anlauf und Betrieb

Anforderungen an Prozeduren und Standards

E6.35 Die Prozeduren für einen sicheren Anlauf und Betrieb müssen erklärt werden. Wenn irgendwelche sicherheitsspezifischen Funktionen während des Anlaufs, des normalen Betriebes oder der Wartung ausgeschaltet oder modifiziert werden können, so muß dies erklärt werden. Verfahren müssen vorhanden sein, die den EVG nach einem Systemausfall oder nach einem Hard- oder Softwarefehler in einen sicheren Zustand zurückversetzen können. Wenn der EVG sicherheitsspezifische Hardware-Komponenten enthält, dann müssen hierfür Diagnoseeinrichtungen vorhanden sein, die durch den

Administrator, den Benutzer oder selbsttätig in der Einsatzumgebung aktiviert werden können.

Anforderungen an Nachweise

E6.36 Die vorgelegten Informationen müssen erklären, wie die Prozeduren die Sicherheit aufrechterhalten. Der Antragsteller muß Beispiele von Ergebnissen aller Diagnoseprozeduren der in Hardware implementierten sicherheitsspezifischen Komponenten zur Verfügung stellen. Der Antragsteller muß Beispiele aller Protokollaufzeichnungen vorlegen, die während des Anlaufs und des Betriebes erstellt werden.

Aufgaben des Evaluators

E6.37 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Die beispielhaften Nachweise für den Anlauf und den Betrieb sind zu überprüfen. Es ist nach Fehlern in den Prozeduren zu suchen.

5 Ergebnisse der Evaluation

Einleitung

5.1 Die Evaluation eines EVG in Übereinstimmung mit den im vorliegenden Dokument enthaltenen Korrektheits- und Wirksamkeitskriterien liefert einen Maßstab für die Vertrauenswürdigkeit, daß der EVG sein Sicherheitsziel erreichen wird. Dies wird durch die erreichte Evaluationsstufe und die Bewertung der Mindeststärke der Sicherheitsmechanismen des EVG angezeigt.

Bewertung

5.2 Die dem EVG als Ergebnis der Evaluation verliehene Bewertung setzt sich zusammen aus:

- einem Verweis auf die Sicherheitsvorgaben des EVG, die als Grundlage für die Evaluation verwendet wurden;
- der durch die Bewertung der Korrektheit und der Betrachtung der Wirksamkeit erreichten Evaluationsstufe;
- einer bestätigten Bewertung der Mindeststärke der Sicherheitsmechanismen des EVG.

5.3 Die Sicherheitsvorgaben müssen in einer Weise spezifiziert werden, die für eine Evaluation durch eine unabhängige Stelle geeignet ist und die mit den Kriterien für die angegebene Evaluationsstufe und dem angegebenen Typ des EVG übereinstimmt.

5.4 Die Evaluationsstufen, die zuerkannt werden, sind E0, E1, E2, E3, E4, E5 oder E6.

5.5 Eine bestätigte Bewertung der Mindeststärke darf nur dann vergeben werden, wenn der EVG erfolgreich evaluiert wurde, d.h. wenn er nicht als E0 eingestuft wurde. Die Einstufung darf nur niedrig, mittel oder hoch sein.

5.6 Ein EVG, der alle Korrektheitskriterien für seine angestrebte Evaluationsstufe erfüllt und alle Betrachtungsaspekte für die Wirksamkeit auf dieser Ebene besteht, einschließlich der postulierten Mindeststärke der Mechanismen, erhält die Einstufung bezüglich dieser Evaluationsstufe und der Mindeststärke der Mechanismen.

5.7 Ein EVG, bei dem eine ausnutzbare Schwachstelle gefunden wurde, die nicht im Verlauf der Evaluation behoben wurde, muß von der Evaluation zurückgezogen werden oder erhält die Bewertung E0.

5.8 Ein EVG, der nicht in der Lage ist, ausreichende Nachweise darüber zu erbringen, daß er die Kriterien für die angestrebte Evaluationsstufe erfüllt, aber bei dem keine auswertbaren Schwachstellen gefunden wurden, kann in eine niedrigere Stufe eingestuft werden, in der die fraglichen Nachweise nicht als Erfüllungskriterien gefordert sind. Falls nicht genügend Zeit oder Betriebsmittel zur Verfügung stehen, um den EVG bezüglich der niedrigeren Stufe zu untersuchen oder falls Fragen unbeantwortet bleiben, dann muß der EVG von der Evaluation zurückgezogen oder mit E0 bewertet werden.

5.9 Ein EVG wird eine Evaluation nur dann aus Gründen der Wirksamkeit nicht bestehen, wenn eine auswertbare Schwachstelle gefunden und nicht behoben wurde. In diesem Fall muß der EVG von der Evaluation zurückgezogen oder mit E0 bewertet werden.

5.10 Ein EVG, dem die Stufe E0 zuerkannt wurde, wird keine Bewertung der Mindeststärke der Mechanismen erhalten, weil nachgewiesen wurde, daß die Vertrauenswürdigkeit des EVG nicht ausreichend ist.

5.11 Der Bericht, der vom Evaluator erstellt wird und der die Evaluationsergebnisse enthält und begründet, muß der zuständigen nationalen Zertifizierungsbehörde in einer geeigneten Form vorgelegt werden.

_____

6 GLOSSAR UND LITERATURVERZEICHNIS *)

Einleitung

6.1 Dieses Kapitel enthält Definitionen technischer Begriffe, die mit einer Bedeutung verwendet werden, die für dieses vorliegende Dokument spezifisch ist. In diesem Dokument verwendete technische Begriffe, die im Glossar nicht definiert sind, werden im Dokument durchgehend mit ihrer allgemein akzeptierten Bedeutung verwendet.

Definitionen

6.2 **Abnahme-Verfahren**: Ein Verfahren, das Objekte, die während des Entwicklungs-, Produktions- und Wartungsprozesses eines Evaluationsgegenstandes erstellt wurden, eindeutig in ein Konfigurationskontrollsystem zur Kontrolle einbezieht.

6.3 **Akkreditierung**: Hat je nach den Umständen zwei Definitionen:

a) das Verfahren, welches ein IT-System zum Betrieb in einer speziellen Umgebung freigibt;

b) das Verfahren, welches für ein Prüflabor gleichzeitig die technische Kompetenz und die Unabhängigkeit, die zugehörigen Aufgaben durchzuführen, anerkennt.

6.4 **Systemverwalter-Dokumentation**: Die vom Entwickler eines Evaluationsgegenstandes gelieferten Informationen zur Verwendung durch den Systemverwalter.

6.5 **Systemverwalter**: Eine Person, die für die Erhaltung der Betriebsbereitschaft des Evaluationsgegenstandes verantwortlich ist.

6.6 **Architekturentwurf**: Eine Phase des Entwicklungsprozesses, in welcher die Top-Level-Definition und der Entwurf eines Evaluationsgegenstandes spezifiziert wird.

6.7 **Vertrauenswürdigkeit**: Eigenschaft des Evaluationsgegenstandes, die das Maß an Vertrauen ausdrückt, welches man in die durch den Evaluationsgegenstand bereitgestellte Sicherheit haben kann.

6.8 **Vertrauenswürdigkeits-Profil**: Eine Anforderung an den Evaluationsgegenstand, wobei an unterschiedliche sicherheitsspezifische Funktionen unterschiedliche Vertrauensanforderungen gestellt werden.

6.9 **Verfügbarkeit**: Eigenschaft eines Objekts, die ausdrückt, inwieweit die unbefugte Zurückhaltung von Informationen oder Betriebsmitteln verhindert werden kann.

*) Die Sortierung der Begriffe entspricht dem englischen Original, sie ist also hier nicht alphabetisch!

6.10 **Basiskomponente:** Eine Komponente, die auf der untersten hierarchischen Stufe des Feinentwurfs identifizierbar ist.

6.11 **Zusammenwirken der Funktionalität:** Ein Aspekt der Bewertung der Wirksamkeit eines Evaluationsgegenstandes, um festzustellen, ob die sicherheitsspezifischen Funktionen und Mechanismen sich gegenseitig unterstützen und ein integriertes und wirksames Ganzes bilden.

6.12 **Zertifizierung:** Die Abgabe einer formalen Erklärung, die die Ergebnisse einer Evaluation und die ordnungsgemäße Anwendung der benutzten Evaluationskriterien bestätigt.

6.13 **Zertifizierungsstelle:** Eine unabhängige und neutrale nationale Stelle, die Zertifizierungen durchführt.

6.14 **Komponente:** Ein identifizierbarer und in sich geschlossener Teil eines Evaluationsgegenstandes.

6.15 **Vertraulichkeit:** Eigenschaft eines Objekts, die ausdrückt, inwieweit die unbefugte Offenlegung von Informationen verhindert werden kann.

6.16 **Konfiguration:** Die Auswahl einer in sich geschlossenen und funktionsfähigen Kombination von Komponenten eines Evaluationsgegenstandes.

6.17 **Konfigurationskontrolle:** Ein System von Kontrollen, welches die Änderung von Objekten betrifft, die während des Entwicklungs-, Produktions- und Wartungsprozesses eines Evaluationsgegenstandes entstehen.

6.18 **Konstruktion:** Der Prozess der Erstellung eines Evaluationsgegenstandes.

6.19 **Firmenspezifische Sicherheitspolitik:** Die Sammlung von Gesetzen, Regeln und Praktiken, die vorschreiben, in welcher Weise Vermögenswerte einschließlich sensitiver Informationen innerhalb einer Benutzerorganisation behandelt, geschützt und verteilt werden.

6.20 **Korrektheit:** Die Eigenschaft eines Evaluationsgegenstandes, die in den Sicherheitsvorgaben des betreffenden Systems oder Produkts aufgeführten Eigenschaften korrekt widerzuspiegeln.

6.21 **Verdeckter Kanal:** Die Nutzung eines Mechanismus, der nicht zur Informationsübermittlung vorgesehen ist, für die Übertragung von Informationen, so daß die Sicherheit verletzt wird.

6.22 **Kritischer Mechanismus:** Ein Mechanismus innerhalb eines Evaluationsgegenstandes, dessen Ausfall eine Sicherheitslücke schaffen würde.

6.23 **Kunde:** Die Person oder Organisation, die einen Evaluationsgegenstand erwirbt.

6.24 **Auslieferung:** Der Prozeß, durch welchen eine Kopie eines Evaluationsgegenstandes vom Entwickler zum Kunden transportiert wird.

6.25 **Feinentwurf:** Eine Phase des Entwicklungsprozesses, in welcher der Architekturentwurf eines Evaluationsgegenstandes verfeinert und auf eine Detailstufe erweitert wird, die als Basis für die Implementierung verwendet werden kann.

6.26 **Entwickler:** Die Person oder Organisation, die einen Evaluationsgegenstand herstellt.

6.27 **Sicherheit beim Entwickler:** Die materiellen, organisatorischen und personellen Sicherheitskontrollen, die ein Entwickler seiner Entwicklungsumgebung auferlegt.

6.28 **Entwicklungsumgebung:** Alle Maßnahmen, Verfahren und Standards, die bei der Konstruktion des Evaluationsgegenstandes getroffen bzw. verwendet werden.

6.29 **Entwicklungsprozeß:** Die Menge von Phasen und Aufgaben, durch welche ein Evaluationsgegenstand mittels Umsetzung der Anforderungen in aktuelle Hard- und Software realisiert wird.

6.30 **Dokumentation:** Die schriftlichen (oder in anderer Weise festgehaltenen) Informationen über einen Evaluationsgegenstand, die für eine Evaluation erforderlich sind. Diese Informationen können (müssen aber nicht) in einem einzigen Dokument enthalten sein, welches für den angegebenen Zweck erstellt wird.

6.31 **Benutzerfreundlichkeit:** Ein Aspekt für die Bewertung der Wirksamkeit eines Evaluationsgegenstandes; insbesondere ist dabei zu gewährleisten, daß der Evaluationsgegenstand nicht in einer Art und Weise konfiguriert oder benutzt werden kann, die unsicher ist, von der aber ein Systemverwalter oder ein Endnutzer glauben könnten, daß sie sicher ist.

6.32 **Wirksamkeit:** Eine Eigenschaft eines Evaluationsgegenstandes, die angibt, wieviel Sicherheitsfunktionalität der Evaluationsgegenstand im Zusammenhang mit seiner tatsächlichen oder vorgesehenen betrieblichen Verwendung bietet.

6.33 **Endnutzer:** Die Person, die den Kontakt zu einem im Betrieb befindlichen Evaluationsgegenstand hat und die seine Dienstleistungen und Funktionen benutzt.

6.34 **Evaluation:** Die Bewertung eines IT-Systems oder -Produkts anhand definierter Evaluationskriterien.

6.35 **Evaluator:** Die unabhängige Person oder Organisation, die eine Evaluation durchführt.

6.36 **Aufgaben des Evaluators:** Vorschriften innerhalb der Evaluationskriterien für eine bestimmte Phase oder einen Aspekt der Evaluation, die angeben, was der Evaluator tun muß, um die vom Antragsteller der Evaluation zur Verfügung gestellten Informationen zu überprüfen und welche sonstigen Aktivitäten er durchführen muß.

6.37 **Formales Sicherheitsmodell:** Ein formal präzise dargestelltes Sicherheitsmodell, d.h. eine abstrakte Aussage der wichtigen Prinzipien der Sicherheit, die ein Evaluationsgegenstand durchsetzen soll.

6.38 **Funktionseinheit:** Ein funktional geschlossener Teil einer Basiskomponente.

6.39 **Funktionalitätsklasse:** Eine vordefinierte Menge von sich ergänzenden sicherheitsspezifischen Funktionen, die in einem Evaluationsgegenstand implementiert werden können.

6.40 **Implementierung:** Eine Phase des Entwicklungsprozesses, in welcher der Feinentwurf eines Evaluationsgegenstandes in reale Hardware und Software umgesetzt wird.

6.41 **Integrität:** Eigenschaft eines Objekts, die ausdrückt, inwieweit unbefugte Änderungen von Informationen verhindert werden können.

6.42 **Objekt:** Eine passive Einheit, die Informationen enthält oder empfängt.

6.43 **Betriebsprozedur:** Eine Reihe von Regeln, die die korrekte Benutzung des Evaluationsgegenstandes festlegen.

6.44 **Betrieb:** Der Vorgang der Nutzung des Evaluationsgegenstandes.

6.45 **Betriebsdokumentation:** Die vom Entwickler eines Evaluationsgegenstandes erstellte Dokumentation zur Spezifizierung und Erläuterung der Art und Weise, in der Kunden das Evaluationsgegenstand verwenden sollten.

6.46 **Betriebsumgebung:** Alle Maßnahmen, Verfahren und Standards, die beim Betrieb des Evaluationsgegenstandes getroffen bzw. verwendet werden.

6.47 **Penetrationstest:** Vom Evaluator durchgeführte Tests des Evaluationsgegenstandes, um festzustellen, ob bekannte Schwachstellen im praktischen Betrieb ausnutzbar sind.

6.48 **Produkt:** Ein Paket aus IT-Software und/oder -Hardware, das eine bestimmte Funktionalität bietet, die zur Verwendung oder zur Integration in einer Vielzahl von Systemen entworfen wurde.

6.49 **Produkt-Beschreibung:** Eine Beschreibung der Fähigkeiten eines Produktes, welche einem zukünftigen Käufer die notwendigen Informationen zur Verfügung stellt, zu entscheiden, ob es hilft, seine System-Sicherheitsziele zu erreichen.

6.50 **Produktion:** Der Vorgang, bei dem Kopien des Evaluationsgegenstandes zum Vertrieb an Kunden erzeugt werden.

6.51 **Programmiersprachen und Compiler:** Hilfsmittel, die innerhalb der Entwicklungsumgebung bei der Realisierung der Software und/oder Firmware des Evaluationsgegenstandes benutzt werden.

6.52 **Bewertung:** Maß für die Vertrauenswürdigkeit, die ein Evaluationsgegenstand bietet und die sich zusammensetzt aus einer Bezugnahme auf die Sicherheitsvorgaben, einer Bewertung der Korrektheit seiner Implementierung und einer Betrachtung seiner Wirksamkeit im Zusammenhang mit dem tatsächlichen oder vorgesehenen Betrieb, sowie aus der Bewertung der Mindeststärke seiner Sicherheitsmechanismen.

6.53 **Anforderungen:** Eine Phase des Entwicklungsprozesses, in der u.a. die Sicherheitsvorgaben eines Evaluationsgegenstandes erstellt werden.

6.54 **Anforderungen an Inhalt und Form:** Ein Bestandteil der Evaluationskriterien für eine bestimmte Phase oder einen bestimmten Aspekt der Evaluation, in welchem definiert wird, welchen Inhalt diejenigen Positionen der Dokumentation, die als relevant für die jeweilige Phase oder den jeweiligen Aspekt der Evaluation identifiziert wurden, haben müssen und wie diese Informationen darzustellen sind.

6.55 **Anforderungen an Nachweise:** Ein Bestandteil der Evaluationskriterien für eine bestimmte Phase oder einen bestimmten Aspekt der Evaluation, durch welchen die Art der Nachweise definiert wird, mit denen aufgezeigt wird, daß die Kriterien für die jeweilige Phase oder den jeweiligen Aspekt erfüllt wurden.

6.56 **Anforderungen an Prozeduren und Standards:** Ein Bestandteil der Evaluationskriterien für eine bestimmte Phase oder einen bestimmten Aspekt der Evaluation, in welchem die Art und/oder der Inhalt von Prozeduren oder Standards definiert werden, die für den praktischen Betrieb des Evaluationsgegenstandes zu übernehmen bzw. zu verwenden sind.

6.57 **Sicherheit:** Die Kombination aus Vertrauenswürdigkeit, Integrität und Verfügbarkeit.

6.58 **Sicherheitsspezifisch:** Das was unmittelbar zur Durchsetzung der Sicherheit beiträgt.

6.59 **Sicherheitsmechanismus:** Die Logik oder der Algorithmus, die eine bestimmte sicherheitsspezifische oder sicherheitsrelevante Funktion in Hard- und Software implementiert.

6.60 **Sicherheitsziele:** Der Beitrag zur Sicherheit, den ein Evaluationsgegenstand leisten soll.

6.61 **Sicherheitspolitik:** Siehe Firmenspezifische Sicherheitspolitik, System-Sicherheitspolitik, Technische Sicherheitspolitik

6.62 **Sicherheitsrelevant:** Das was nicht sicherheitsspezifisch ist, jedoch korrekt funktionieren muß, damit der Evaluationsgegenstand die Sicherheit garantieren kann.

6.63 **Sicherheitsvorgaben:** Eine Spezifikation der von einem Evaluationsgegenstand geforderten Sicherheit, die als Grundlage für die Evaluation verwendet wird. Die Sicherheitsvorgaben spezifizieren die sicherheitsspezifischen Funktionen des Evaluationsgegenstandes. Sie spezifizieren auch die Sicherheitsziele, die Bedrohungen dieser Ziele sowie die einzelnen Sicherheitsmechanismen, die verwendet werden.

6.64 **Antragsteller:** Die Person oder Organisation, die die Evaluation beantragt.

6.65 **Speicherobjekt:** Ein Objekt, das sowohl Lese- wie Schreibzugriffe ermöglicht [TCSEC].

6.66 **Stärke der Mechanismen:** Ein Aspekt der Bewertung der Wirksamkeit eines Evaluationsgegenstandes; drückt die Fähigkeit seiner Sicherheitsmechanismen aus, direkten Angriffen gegen ihre zugrundeliegenden Algorithmen, Prinzipien und Eigenschaften zu widerstehen.

6.67 **Subjekt:** Eine aktive Einheit, normalerweise in der Form einer Person, eines Prozesses oder von Geräten [TCSEC].

6.68 **Eignung der Funktionalität:** Ein Aspekt der Bewertung der Wirksamkeit eines Evaluationsgegenstandes; drückt aus, inwieweit die sicherheitsspezifischen Funktionen und Mechanismen dieses Evaluationsgegenstandes in der Praxis den tatsächlichen oder möglichen, in seinen Sicherheitsvorgaben identifizierten Bedrohungen der Sicherheit des Evaluationsgegenstandes entgegenwirken.

6.69 **System:** Eine spezifische IT-Installation mit einem bestimmten Zweck und einer spezifischen Betriebsumgebung.

6.70 **System-Sicherheitspolitik:** Die Sammlung von Gesetzen, Regeln und Praktiken, die vorschreiben, in welcher Weise sensitive Informationen und andere Betriebsmittel innerhalb eines bestimmten Systems behandelt, geschützt und verteilt werden.

6.71 **Evaluationsgegenstand (EVG):** Ein IT-System oder -Produkt, das einer Evaluation unterzogen wird.

6.72 **Technische Sicherheitspolitik:** Die Menge der Gesetze, Regeln und Praktiken, die die Verarbeitung von sensitiven Informationen und die Nutzung von Betriebsmitteln durch die Hard- und Software eines IT-System oder -Produkts festlegen.

6.73 **Bedrohung:** Eine Aktion oder ein Ereignis, das der Sicherheit schaden kann.

6.74 **Werkzeug:** Ein Produkt, das bei der Entwicklung (auch bei der Dokumentation) eines Evaluationsgegenstandes eingesetzt wird.

6.75 **Benutzerdokumentation:** Die vom Entwickler zur Verwendung durch die Endbenutzer bereitgestellten Informationen über einen Evaluationsgegenstand.

6.76 **Schwachstelle:** Eine Sicherheitsschwäche in einem Evaluationsgegenstand (z.B. durch Fehler in der Analyse, Entwurf, Implementierung oder Betrieb).

6.77 **Schwachstellenbewertung:** Ein Aspekt der Bewertung der Wirksamkeit eines Evaluationsgegenstandes; drückt aus, inwieweit bekannte Schwachstellen des Evaluationsgegenstandes seine Sicherheit, wie sie in den Sicherheitsvorgaben spezifiziert ist, beeinträchtigen können.

Claims:[*])

- aus der Sicht des Endnutzers:
  Anforderungen bzgl. bestimmter Eigenschaften von Komponenten, Funktionen und Mechanismen.
- aus der Sicht des Evaluators:
  Aussagen bzgl. der Existenz von Eigenschaften in Komponenten, Funktionen und Mechanismen.

Literaturverzeichnis

6.78 Die folgenden Bücher und Arbeiten werden im Text zitiert:

AND Computer Security Technology Planning Study
J. P. Anderson
ESD-TR-73-51, ESD/AFSC, US Air Force, Bedford, Mass., October 1972.

BLP Secure Computer Systems: Unified Exposition and Multics Interpretation
D.E. Bell and L.J. LaPadula
Report MTR-2997 Rev. 1, MITRE Corporation, Bedford, Mass, 1976.

BNM The Chinese Wall Security Policy
D.F.C. Brewer and M.J. Nash
Proceedings of the IEEE Symposium on Security and Privacy, Oakland, May 1989, pp. 206-214.

CESG3 UK Systems Security Confidence Levels, CESG Memorandum No. 3,
Communications-Electronics Security Group, United Kingdom, January 1989.

CWM A Comparison of Commercial and Military Computer Security Policies
D. D. Clark and D. R. Wilson
Proceedings of the IEEE Symposium on Security and Privacy, Oakland, April 1987, pp. 184-194.

[*]) Dieser Begriff ist nur in der deutschen Übersetzung erläutert und erhält somit keine Nummer.

DTIEC DTI Commercial Computer Security Centre Evaluation Levels Manual, V22
Department of Trade and Industry, United Kingdom, February 1989.

DTIFN DTI Commercial Computer Security Centre Security Functionality Manual, V21
Department of Trade and Industry, United Kingdom, February 1989.

EZBM Mandatory Policy: Secure Systems Model
G. Eizenberg
ONERA/CERT/DERI, Toulouse, France, undated.

GYPSY Report on Gypsy 2.05
D.I. Good, R.L. Akers and L.M. Smith
Report ICSCA-CMP-48, University of Texas at Austin, February 1986.

IJRM The Ina Jo Specification Language Reference Manual
Unisys Corporation
Culver City, California, United States of America, 1989.

JSD System Development
M.A. Jackson
Prentice-Hall International, 1983.

JSP Principles of Program Design
M.A. Jackson
Academic Press, New York, 1975

LOTOS Information Processing Systems - Open Systems Interconnection - LOTOS -
A Formal Description Technique Based on the Temporal Ordering of
Observational Behaviour
International Standard ISO 8807
International Organization for Standardization, 1989.

LWM A Security Model for Military Message Systems
C.E. Landwehr, C.L. Heitmeyer and J. McLean
ACM Transactions on Computer Systems, Vol. 2 No. 3, August 1984,
pp. 198-222.

OSI Information Processing Systems - Open Systems Interconnection - Basic
Reference Model - Part 2: Security Architecture
International Standard ISO 7498-2
International Organization for Standardization, 1988.

RSL RAISE Specification Language Reference Manual,
RAISE/CRI/DOC/2/V1
Computer Resources International A/S
Birker·d, Denmark, 1990.

SADT An Introduction to SADT
Structured Analysis and Design Technique
Report 9022-78R
SofTech Inc, 460 Totten Pond Road
Waltham, MA 02154, USA, November 1976.

SCSSI Catalogue de Critères Destinés à évaluer le Degré de Confiance des Systèmes d'Information, 692/SGDN/DISSI/SCSSI
Service Central de la Sécurité des Systèmes d'Information, Juillet 1989.

SSADM The SSADM Manual, ISBN 085-012-527-X
National Computing Centre Limited
Manchester, United Kingdom, 1989.

SSVDM Systematic Software Development Using VDM
C.B. Jones
Prentice Hall International, 1990.

TCSEC Trusted Computer Systems Evaluation Criteria, DOD 5200.28-STD,
Department of Defense, United States of America, December 1985.

YSM A Note on the Yourdon Structured Method
A.J. Bowles
Yourdon Inc
ACM SIGSOFT Software Engineering Notes
Vol. 15 No. 2 April 1990, p. 27.

ZRM The Z Notation: A Reference Manual, ISBN-0-13-983768-X
J.M. Spivey
Prentice Hall International, 1988.

ZSIEC Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems, ISBN 3-88784-200-6
German Information Security Agency (Bundesamt für Sicherheit in der Informationstechnik), Federal Republic of Germany, January 1989.

Anhang A - Beispiele von Funktionalitätsklassen

Einleitung

A.1 Dieser Anhang enthält Beispiele von vordefinierten Funktionalitätsklassen, so wie in Kapitel 2 definiert. Diese Klassen befinden sich im Anhang der Kriterien, da sie als Beispiele gedacht sind und nicht als die letztgültigen Klassen, die in echten Evaluationen Verwendung finden. Es ist zu erhoffen, daß sie die Diskussion über aktuelle Anforderungen an Sicherheitsfunktionalität fördern. Während des Abstimmungsprozesses, der der Veröffentlichung der vorliegenden Version vorausging, hat die Notwendigkeit, festgeschriebene vordefinierte Funktionalitätsklassen zu erarbeiten, tatsächlich breite Zustimmung gefunden.

A.2 Standardisierungsgremien und Industrieorganisationen sind schon dabei, Standards für die Sicherheitsfunktionalität in bestimmten Bereichen zu entwickeln. Es ist vorherzusehen, daß diese Arbeit allgemein akzeptierte Definitionen von Sicherheitsfunktionalität hervorbringt, die zur Anwendung im Rahmen dieser Kriterien angepaßt werden können und die in der nächsten Version dieses Dokumentes mit eingeschlossen werden oder auf die verwiesen wird.

A.3 Die jetzigen Beispiele stellen einen Referenzpunkt dar und zeigen, wie vordefinierte Funktionalitätsklassen aus vorhandenen Kriterien fortentwickelt werden können: tatsächlich stammen die Klassen mit geringen Änderungen aus [ZSIEC].

A.4 Jede Klasse besteht aus einer Aussage zur Zielsetzung, gefolgt von den Anforderungen unter den entsprechenden generischen Oberbegriffen. Die Abwesenheit eines generischen Oberbegriffs innerhalb einer Klasse sagt aus, daß hierfür keine Anforderungen bestehen. Die Klassen F-B2 und F-B3 enthalten noch weitere Informationen, die als Teil der Sicherheitsvorgaben notwendig sind. Diese Informationen betreffen die zur Kompatibilität mit den TCSEC notwendigen Sicherheitsmechanismen.

A.5 Die fünf Beispiele der Funktionalitätsklassen F-C1, F-C2, F-B1, F-B2 und F-B3 bilden eine Hierarchie, da sie von den Funktionalitätsanforderungen der hierarchischen TCSEC-Klassen abgeleitet wurden. In der Beschreibung dieser Klassen sind jene Teile, die sich gegenüber der vorhergehenden Klasse geändert haben oder neu hinzukommen, fett gedruckt.

A.6 Andere hierarchisch aufgebaute Funktionalitätsklassen können in der Zukunft durch Standardisierungsgremien oder Industrieorganisationen entstehen, um andere Sicherheitsziele zu adressieren (z.B. hinsichtlich Integrität und Verfügbarkeit). In der Zwischenzeit sind die Beispielklassen F-IN, F-AV, F-DI, F-DC und F-DX eingefügt worden, um die breite Palette an Sicherheitsanforderungen, die in Form von vordefinierten Funktionalitätsklassen ausgedrückt werden können, aufzuzeigen.

Beispiel: Funktionalitätsklasse F-C1

Zielsetzung

A.7 Die Beispielklasse F-C1 ist von den Funktionalitätsanforderungen der US-TCSEC-Klasse C1 abgeleitet. Sie stellt benutzerbestimmbare Zugriffskontrollen zur Verfügung ("Kenntnis nur wenn nötig").

Identifikation und Authentisierung

A.8 Der EVG muß Benutzer identifizieren und authentisieren. Diese Identifikation und Authentisierung muß vor jeder anderen Interaktion des EVG mit dem Benutzer erfolgen. Weitere Interaktionen dürfen nur nach der erfolgreichen Identifikation und Authentisierung möglich sein. Die Authentisierungsinformationen müssen so gespeichert sein, daß nur autorisierte Benutzer darauf Zugriff haben.

Zugriffskontrolle

A.9 Der EVG muß in der Lage sein, Zugriffsrechte von jedem Benutzer auf Objekte, die der Rechteverwaltung unterliegen, zu unterscheiden und zu verwalten. Dies geschieht auf der Basis eines einzelnen Benutzers oder der Zugehörigkeit zu einer Benutzergruppe oder beidem. Es muß möglich sein, Benutzern bzw. Benutzergruppen den Zugriff auf ein Objekt ganz zu verwehren. Keine Person außer einem autorisierten Benutzer darf die Möglichkeit haben, Rechte bzgl. eines Objektes zu vergeben oder zu entziehen.

A.10 Bei jedem Zugriffsversuch von Benutzern bzw. Benutzergruppen auf Objekte, die der Rechteverwaltung unterliegen, hat der EVG die Berechtigung der Anforderung zu überprüfen. Unberechtigte Zugriffsversuche müssen abgewiesen werden.

Beispiel: Funktionalitätsklasse F-C2

Zielsetzung

A.11 **Die Beispielklasse F-C2 ist von den Funktionalitätsanforderungen der US-TCSEC-Klasse C2 abgeleitet. Sie stellt eine feinere benutzerbestimmbare Zugriffskontrolle als die Klasse F-C1 zur Verfügung. Sie stellt die Verantwortlichkeit der Benutzer für ihre Aktionen sicher mit Hilfe von Identifizierungsverfahren, Protokollierung von sicherheitsrelevanten Ereignissen und Trennung von Betriebsmitteln.**

Identifikation und Authentisierung

A.12 Der EVG muß Benutzer **eindeutig** identifizieren und authentisieren. Diese Identifikation und Authentisierung muß vor jeder anderen Interaktion des EVG mit dem Benutzer erfolgen. Weitere Interaktionen dürfen nur nach der erfolgreichen Identifikation und Authentisierung möglich sein. Die Authentisierungsinformationen müssen so gespeichert sein, daß nur autorisierte Benutzer darauf Zugriff haben. **Bei jeder Interaktion muß der EVG die Identität des Benutzers feststellen können.**

Zugriffskontrolle

A.13 Der EVG muß in der Lage sein, Zugriffsrechte von jedem Benutzer auf Objekte, die der Rechteverwaltung unterliegen, zu unterscheiden und zu verwalten. Dies geschieht auf der Basis eines einzelnen Benutzers oder der Zugehörigkeit zu einer Benutzergruppe oder beidem. Es muß möglich sein, Benutzern bzw. Benutzergruppen den Zugriff auf ein Objekt ganz zu verwehren. **Daneben muß es ebenfalls möglich sein, den Zugriff eines Benutzers auf ein Objekt auf nichtmodifizierende Operationen einzuschränken. Es muß möglich sein, für jeden Benutzer einzeln die Zugriffsrechte bzgl. eines Objektes zu erteilen.** Keine Person außer einem autorisierten Benutzer darf die Möglichkeit haben, Rechte bzgl. eines Objektes zu vergeben oder zu entziehen. **Die Rechteverwaltung muß die Weitergabe von Zugriffsrechten kontrollieren. Ebenso darf das Einbringen neuer Benutzer sowie das Löschen bzw. Sperren von Benutzern nur durch autorisierte Benutzer möglich sein.**

A.14 Bei jedem Zugriffsversuch von Benutzern bzw. Benutzergruppen auf Objekte, die der Rechteverwaltung unterliegen, hat der EVG die Berechtigung der Anforderung zu überprüfen. Unberechtigte Zugriffsversuche müssen abgewiesen werden.

Beweissicherung

A.15 **Der EVG muß eine Protokollierungskomponente enthalten, die in der Lage ist, jedes der folgenden Ereignisse mit den angegebenen Daten zu protokollieren:**

a) Benutzung des Identifikations- und Authentisierungsmechanismus:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id., die angegeben wurde; Kennung des Gerätes, an dem der Identifikations- und Authentisierungsmechanismus benutzt wurde (z.B. Terminal-Id.); Erfolg bzw. Mißerfolg des Versuchs.

b) Versuchter Zugriff auf ein der Rechteverwaltung unterliegendes Objekt:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Name des Objekts; Art des versuchten Zugriffs; Erfolg bzw. Mißerfolg des Versuchs.

d) Aktionen von authorisierten Benutzern, die die Sicherheit des EVG betreffen:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Art der Aktion; Name des Objektes, auf das sich die Aktion bezog (Solche Aktionen sind z.B. das Einbringen oder Löschen (Sperren) von Benutzern; Einbringen oder Entfernen von Datenträgern; Starten bzw. Stoppen des EVG).

A.16 **Der Zugriff auf Protokollinformation darf nur dazu autorisierten Benutzern möglich sein. Es muß möglich sein, die Beweissicherung auf einen oder mehrere Benutzer zu beschränken. Werkzeuge zur Auswertung und Verwaltung von Protokolldaten müssen vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, selektiv die Aktionen eines oder mehrerer Benutzer zu identifizieren.**

Protokollauswertung

A.17 **Es müssen Werkzeuge zur Überprüfung der Protokolldateien zu Revisionszwecken vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, selektiv die Aktionen eines oder mehrerer Benutzer zu identifizieren.**

Wiederaufbereitung

A.18 **Alle Speicherobjekte, die dem EVG wieder zur Verfügung gestellt werden, müssen vor einer Wiederverwendung durch andere Benutzer so aufbereitet werden, daß keine Rückschlüsse auf ihren früheren Inhalt möglich sind.**

Beispiel: Funktionalitätsklasse F-B1

Zielsetzung

A.19 **Die Beispielklasse F-B1 ist von den Funktionalitätsanforderungen der US-TCSEC-Klasse B1 abgeleitet. Zusätzlich zur benutzerbestimmbaren Zugriffskontrolle führt sie Funktionen zur Verwaltung von Sensitivitätsattributen ein. Diese werden verwendet, um einen Satz von vorgeschriebenen Zugriffskontrollregeln bezüglich aller kontrollierten Subjekte und Speicherobjekte durchzusetzen. Es ist möglich, nach außen gehende Informationen mit korrekten Attributen zu versehen.**

Identifikation und Authentisierung

A.20 Der EVG muß Benutzer eindeutig identifizieren und authentisieren. Diese Identifikation und Authentisierung muß vor jeder anderen Interaktion des EVG mit dem Benutzer erfolgen. Weitere Interaktionen dürfen nur nach der erfolgreichen Identifikation und Authentisierung möglich sein. Die Authentisierungsinformationen müssen so gespeichert sein, daß nur autorisierte Benutzer darauf Zugriff haben. Bei jeder Interaktion muß der EVG die Identität des Benutzers feststellen können.

Zugriffskontrolle

A.21 Der EVG muß in der Lage sein, Zugriffsrechte von jedem Benutzer auf Objekte, die der Rechteverwaltung unterliegen, zu unterscheiden und zu verwalten. Dies geschieht auf der Basis eines einzelnen Benutzers oder der Zugehörigkeit zu einer Benutzergruppe oder beidem. Es muß möglich sein, Benutzern bzw. Benutzergruppen den Zugriff auf ein Objekt ganz zu verwehren. Daneben muß es ebenfalls möglich sein, den Zugriff eines Benutzers auf ein Objekt auf nichtmodifizierende Operationen einzuschränken. Es muß möglich sein, für jeden Benutzer einzeln die Zugriffsrechte bzgl. eines Objektes zu erteilen. Keine Person außer einem autorisierten Benutzer darf die Möglichkeit haben, Rechte bzgl. eines Objektes zu vergeben oder zu entziehen. Die Rechteverwaltung muß die Weitergabe von Zugriffsrechten kontrollieren. Ebenso darf das Einbringen neuer Benutzer, das Löschen von Benutzern sowie das zeitweilige Sperren aller Rechte eines Benutzers nur durch autorisierte Benutzer möglich sein.

A.22 **Daneben muß der EVG alle Subjekte und Speicherobjekte (z.B. Prozesse, Dateien, Speichersegmente, Geräte), die seiner Kontrolle unterliegen, mit Attributen versehen. Der Wert dieser Attribute muß dabei als Grundlage für obligatorische Zugriffsrechte dienen. Es muß durch Regeln festgelegt werden, welche Kombination der Attributwerte von Subjekt und Objekt für ein Subjekt nötig ist, um Zugriff auf dieses Objekt zu erhalten.**

A.23 **Beim Export eines Objekts müssen die Attribute so mitexportiert werden, daß der Empfänger ihren Wert eindeutig rekonstruieren kann.**

A.24 **Die obligatorischen Zugriffsrechte müssen so gestaltet sein, daß der folgende Sonderfall realisiert werden kann:**

Das Attribut besteht aus zwei Teilen. Der erste Teil besitzt hierarchisch geordnete Werte, der zweite stellt eine Menge dar. (Im Amtsbereich enthält der erste Teil Einstufungen, z.B. offen, vertraulich, geheim, streng geheim. Der zweite Teil enthält Kategorien.)

Ein Attribut A dominiert Attribut B genau dann, wenn:

Teil 1 von A hierarchisch größer oder gleich Teil 1 von B ist
und Teil 2 von B eine echte Teilmenge von oder gleich Teil 2 von A ist.

A.25 **Die folgenden Regeln müssen durchgesetzt werden:**

a) Lesender Zugriff eines Subjekts auf ein Objekt ist nur gestattet, wenn das Attribut des Subjekts das des Objekts dominiert.

b) Schreibender Zugriff eines Subjekts auf ein Objekt ist nur gestattet, wenn das Attribut des Objekts das des Subjekts dominiert.

A.26 **Die Attribute eines Subjekts, das für einen Benutzer aktiv wird, werden dominiert durch die Ermächtigung und Autorisierung dieses Benutzers, wie sie zum Zeitpunkt der Identifikation und Authentisierung festgestellt wurde. Wenn importierte Daten keine Attribute besitzen, muß ein autorisierter Benutzer in der Lage sein, diesen Daten Attribute zuzuordnen.**

A.27 **Exportkanäle müssen als einstufig oder mehrstufig identifizierbar sein. Über einen als einstufig gekennzeichneten Kanal dürfen nur Daten gesendet oder empfangen werden, wenn die Attribute dieser Daten mit einem vorab definierten Attribut übereinstimmen. Daten, die an einen einstufigen Kanal gesendet oder von einem einstufigen Kanal empfangen werden, müssen mit einem entsprechenden Attribut versehen werden, wenn es einem autorisierten Benutzer nicht möglich ist, das Attribut des Kanals untäuschbar festzulegen. In diesem Fall wird das Attribut der Daten implizit durch das Attribut des Kanals festgelegt.**

A.28 **Bei mehrstufigen Kanälen muß durch das Übertragungsprotokoll sichergestellt sein, daß die Empfängerseite alle empfangenen Daten und Attribute vollständig und eindeutig rekonstruieren und dabei die Attribute den Daten eindeutig zuordnen kann.**

A.29 **Nichtautorisierten Benutzern muß es unmöglich sein, die sicherheitsrelevanten Attribute eines Kanals zu ändern. Eine Änderung dieser Attribute muß in expliziter Form erfolgen.**

A.30 **Der EVG muß menschenlesbare Ausgaben mit Attributwerten kennzeichnen. Die Werte der Attribute leiten sich aus den im EVG formulierten Regeln ab. Autorisierte Benutzer müssen in der Lage sein, den zu druckenden Namen jedes einzelnen Attributwerts zu spezifizieren.**

A.31 Bei jedem Zugriffsversuch von Benutzern bzw. Benutzergruppen auf Objekte, die der Rechteverwaltung unterliegen, hat der EVG die Berechtigung der Anforderung zu überprüfen. Unberechtigte Zugriffsversuche müssen abgewiesen werden. **Die Werte der Attribute müssen als Grundlage für Entscheidungen bezüglich einer obligatorischen Zugriffskontrolle dienen. Die Regeln müssen eindeutig festlegen, wann ein Subjekt Zugriff auf ein derart geschütztes Objekt hat. Falls für ein Objekt zusätzlich noch benutzerbestimmbare Zugriffsrechte bestehen, darf ein Zugriff nur zugelassen werden, wenn sowohl die benutzerbestimmbaren als auch die obligatorischen Zugriffsrechte diesen Zugriff gestatten.**

Beweissicherung

A.32 Der EVG muß eine Protokollierungskomponente enthalten, die in der Lage ist, jedes der folgenden Ereignisse mit den angegebenen Daten zu protokollieren:

a) Benutzung des Identifikations- und Authentisierungsmechanismus:

   Geforderte Daten: Datum; Uhrzeit; Benutzer-Id., die angegeben wurde; Kennung des Gerätes, an dem der Identifikations- und Authentisierungsmechanismus benutzt wurde (z.B. Terminal-Id.); Erfolg bzw. Mißerfolg des Versuchs; **Autorisierung des Benutzers.**

b) Versuchter Zugriff auf ein der Rechteverwaltung unterliegendes Objekt:

   Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Name des Objekts; Art des versuchten Zugriffs; Erfolg bzw. Mißerfolg des Versuchs; **Attribut des Objekts**.

c) Anlegen bzw. Löschen eines der Rechteverwaltung unterliegenden Objekts:

   Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Name des Objektes; Art der Aktion; **Attribut des Objekts**.

d) Aktionen von authorisierten Benutzern, die die Sicherheit des EVG betreffen:

   Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Art der Aktion; Name **und Attribut** des Objektes, auf das sich die Aktion bezog (Solche Aktionen sind z.B. das Einbringen oder Löschen (Sperren) von Benutzern; Einbringen oder Entfernen

von Datenträgern; Starten bzw. Stoppen des EVG; **Zuordnung eines Attributs; Änderung der Attribute, Kennzeichnungen oder Klassifikation eines Kanals).**

A.33 Der Zugriff auf Protokollinformation darf nur dazu autorisierten Benutzern möglich sein. Es muß möglich sein, die Beweissicherung auf einen oder mehrere Benutzer zu beschränken. Werkzeuge zur Auswertung und Verwaltung von Protokollierungsdaten müssen vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, selektiv die Aktionen eines oder mehrerer Benutzer zu identifizieren.

Protokollauswertung

A.34 Es müssen Werkzeuge zur Überprüfung der Protokolldateien zu Revisionszwecken vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, selektiv die Aktionen eines oder mehrerer Benutzer zu identifizieren.

Wiederaufbereitung

A.35 Alle Speicherobjekte, die dem EVG wieder zur Verfügung gestellt werden, müssen vor einer Wiederverwendung durch andere Benutzer so aufbereitet werden, daß keine Rückschlüsse auf ihren früheren Inhalt möglich sind.

Beispiel: Funktionalitätsklasse F-B2

Zielsetzung

A.36 **Die Beispielklasse F-B2 ist von den Funktionalitätsanforderungen der US-TCSEC-Klasse B2 abgeleitet. Sie erweitert die obligatorische Zugriffskontrolle auf alle Subjekte und Objekte und verstärkt die Anforderungen an die Authentisierung der Klasse F-B1.**

Obligatorische Mechanismen

A.37 **Diese Klasse verlangt, daß die Zugriffskontrolle durch einen einzigen "Referenz-Validierungsmechanismus" realisiert wird, der das "Referenz-Monitor-Konzept" erfüllt, d.h. der Mechanismus ist sicher gegen Veränderungen, immer eingeschaltet und so klein (ausreichend einfach), daß er Analysen und Tests unterzogen werden kann, deren Vollständigkeit garantiert werden kann.**

Identifikation und Authentisierung

A.38 Der EVG muß Benutzer eindeutig identifizieren und authentisieren. Diese Identifikation und Authentisierung muß vor jeder anderen Interaktion des EVG mit dem Benutzer erfolgen. Weitere Interaktionen dürfen nur nach der erfolgreichen Identifikation und Authentisierung möglich sein. Die Authentisierungsinformationen müssen so gespeichert sein, daß nur autorisierte Benutzer darauf Zugriff haben. **Identifikation und Authentisierung müssen über einen vertrauenswürdigen Pfad zwischen Benutzer und EVG abgewickelt werden, initiiert durch den Benutzer.** Bei jeder Interaktion muß der EVG die Identität des Benutzers feststellen können.

Zugriffskontrolle

A.39 Der EVG muß in der Lage sein, Zugriffsrechte von jedem Benutzer auf Objekte, die der Rechteverwaltung unterliegen, zu unterscheiden und zu verwalten. Dies geschieht auf der Basis eines einzelnen Benutzers oder der Zugehörigkeit zu einer Benutzergruppe oder beidem. **Es muß möglich sein, die Zugriffsrechte zur Unterstützung von Rollen in Gruppen zusammenzufassen. Zumindest die Rollen des EVG-Bedieners und -Systemverwalters müssen definierbar sein.** Es muß möglich sein, Benutzern bzw. Benutzergruppen den Zugriff auf ein Objekt ganz zu verwehren. Daneben muß es ebenfalls möglich sein, den Zugriff eines Benutzers auf ein Objekt auf nicht-modifizierende Operationen einzuschränken. Es muß möglich sein, für jeden Benutzer einzeln die Zugriffsrechte bzgl. eines Objektes zu erteilen.

A.40 Keine Person außer einem autorisierten Benutzer darf die Möglichkeit haben, Rechte bzgl. eines Objektes zu vergeben oder zu entziehen. Die Rechteverwaltung muß die Weitergabe von Zugriffsrechten kontrollieren. Ebenso darf das Einbringen neuer Benutzer, das Löschen von Benutzern sowie das zeitweilige Sperren aller Rechte eines Benutzers nur durch autorisierte Benutzer möglich sein.

A.41 Daneben muß der EVG alle Subjekte und **Objekte** (z.B. Prozesse, Dateien, Speichersegmente, Geräte) **mit** Attributen versehen. Der Wert dieser Attribute muß dabei als Grundlage für obligatorische Zugriffsrechte dienen. Es muß durch Regeln festgelegt werden, welche Kombination der Attributwerte von Subjekt und Objekt für ein Subjekt nötig ist, um Zugriff auf dieses Objekt zu erhalten.

A.42 Beim Export eines Objekts müssen die Attribute so mitexportiert werden, daß der Empfänger ihren Wert eindeutig rekonstruieren kann.

A.43 Die obligatorischen Zugriffsrechte müssen so gestaltet sein, daß der folgende Sonderfall realisiert werden kann:

Das Attribut besteht aus zwei Teilen. Der erste Teil besitzt hierarchisch geordnete Werte, der zweite stellt eine Menge dar. (Im Amtsbereich enthält der erste Teil Einstufungen, z.B. offen, vertraulich, geheim, streng geheim. Der zweite Teil enthält Kategorien.)

Ein Attribut A dominiert Attribut B genau dann, wenn:

Teil 1 von A hierarchisch größer oder gleich Teil 1 von B ist
und Teil 2 von B eine echte Teilmenge von oder gleich Teil 2 von A ist.

A.44 Die folgenden Regeln müssen durchgesetzt werden:

a) Lesender Zugriff eines Subjekts auf ein Objekt ist nur gestattet, wenn das Attribut des Subjekts das des Objekts dominiert.

b) Schreibender Zugriff eines Subjekts auf ein Objekt ist nur gestattet, wenn das Attribut des Objekts das des Subjekts dominiert.

A.45 Die Attribute eines Subjekts, das für einen Benutzer aktiv wird, werden dominiert durch die Ermächtigung und Autorisierung dieses Benutzers, wie sie zum Zeitpunkt der Identifikation und Authentisierung festgestellt wurde. Wenn importierte Daten keine Attribute besitzen, muß ein autorisierter Benutzer in der Lage sein, diesen Daten Attribute zuzuordnen.

A.46 Exportkanäle müssen als einstufig oder mehrstufig identifizierbar sein. Über einen als einstufig gekennzeichneten Kanal dürfen nur Daten gesendet oder empfangen werden, wenn die Attribute dieser Daten mit einem vorab definierten Attribut übereinstimmen. Daten, die an einen einstufigen Kanal gesendet oder von einem einstufigen Kanal empfangen werden, müssen mit einem entsprechenden Attribut versehen werden, wenn

es einem autorisierten Benutzer nicht möglich ist, das Attribut des Kanals untäuschbar festzulegen. In diesem Fall wird das Attribut der Daten implizit durch das Attribut des Kanals festgelegt.

A.47 Bei mehrstufigen Kanälen muß durch das Übertragungsprotokoll sichergestellt sein, daß die Empfängerseite alle empfangenen Daten und Attribute vollständig und eindeutig rekonstruieren und dabei die Attribute den Daten eindeutig zuordnen kann. **Für mehrstufige Kanäle muß es möglich sein, den maximalen und minimalen Attributwert anzugeben. Es dürfen keine Daten an einen mehrstufigen Kanal gesendet werden, wenn nicht das Attribut der Daten das Minimalattribut des Kanals dominiert und seinerseits durch das Maximalattribut des Kanals dominiert wird.**

A.48 Nichtautorisierten Benutzern muß es unmöglich sein, die sicherheitsrelevanten Attribute eines Kanals zu ändern. Eine Änderung dieser Attribute muß in expliziter Form erfolgen.

A.49 Der EVG muß menschenlesbare Ausgaben mit Attributwerten kennzeichnen. Die Werte der Attribute leiten sich aus den im EVG formulierten Regeln ab. Autorisierte Benutzer müssen in der Lage sein, den zu druckenden Namen jedes einzelnen Attributwerts zu spezifizieren.

A.50 **Jede Änderung der Sicherheitsstufe, die einem Benutzer während einer laufenden interaktiven Sitzung zugeordnet ist, muß diesem Benutzer sofort angezeigt werden. Der Benutzer muß jederzeit die Möglichkeit haben, sich alle Attribute des Subjekts anzeigen zu lassen.**

A.51 Bei jedem Zugriffsversuch von Benutzern bzw. Benutzergruppen auf Objekte, die der Rechteverwaltung unterliegen, hat der EVG die Berechtigung der Anforderung zu überprüfen. Unberechtigte Zugriffsversuche müssen abgewiesen werden. Die Werte der Attribute müssen als Grundlage für Entscheidungen bezüglich einer obligatorischen Zugriffskontrolle dienen. Die Regeln müssen eindeutig festlegen, wann ein Subjekt Zugriff auf ein derart geschütztes Objekt hat. Falls für ein Objekt zusätzlich noch benutzerbestimmbare Zugriffsrechte bestehen, darf ein Zugriff nur zugelassen werden, wenn sowohl die benutzerbestimmbaren als auch die obligatorischen Zugriffsrechte diesen Zugriff gestatten.

A.52 **Es darf keine bekannten Speicher-Kanäle geben, die Informationen zwischen Prozessen ohne Prüfung von Zugriffsrechten (d.h. verdeckt) übertragen können und die außerdem eine nichtakzeptabel hohe Bandbreite haben (festgestellt durch aktuelle Messung oder ingenieurmäßige Abschätzung). (Bezüglich der Einschätzung von "Akzeptierbarkeit": Siehe auch den Abschnitt zu Covert channel Guidelines in den TCSEC [TCSEC]).**

Beweissicherung

A.53 Der EVG muß eine Protokollierungskomponente enthalten, die in der Lage ist, jedes der folgenden Ereignisse mit den angegebenen Daten zu protokollieren:

a) Benutzung des Identifikations- und Authentisierungsmechanismus:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id., die angegeben wurde; Kennung des Gerätes, an dem der Identifikations- und Authentisierungsmechanismus benutzt wurde (z.B. Terminal-Id.); Erfolg bzw. Mißerfolg des Versuchs; Autorisierung des Benutzers.

b) Versuchter Zugriff auf ein der Rechteverwaltung unterliegendes Objekt:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Name des Objekts; Art des versuchten Zugriffs; Erfolg bzw. Mißerfolg des Versuchs; Attribut des Objekts.

c) Anlegen bzw. Löschen eines der Rechteverwaltung unterliegenden Objekts:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Name des Objektes; Art der Aktion; Attribut des Objekts.

d) Aktionen von autorisierten Benutzern, die die Sicherheit des EVG betreffen:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Art der Aktion; Name und Attribut des Objektes, auf das sich die Aktion bezog (Solche Aktionen sind z.B. das Einbringen oder Löschen (Sperren) von Benutzern; Einbringen oder Entfernen von Datenträgern; Starten bzw. Stoppen des EVG; Zuordnung eines Attributs; Änderung der Attribute, Kennzeichnungen oder Klassifikation eines Kanals).

A.54 Der Zugriff auf Protokollinformation darf nur dazu autorisierten Benutzern möglich sein. Es muß möglich sein, die Beweissicherung auf einen oder mehrere Benutzer zu beschränken. Werkzeuge zur Auswertung und Verwaltung von Protokolldaten müssen vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, selektiv die Aktionen eines oder mehrerer Benutzer zu identifizieren.

Protokollauswertung

A.55 Es müssen Werkzeuge zur Überprüfung der Protokolldateien zu Revisionszwecken vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, selektiv die Aktionen eines oder mehrerer Benutzer zu identifizieren. **Zusätzlich muß der EVG in der Lage sein, bekannte Ereignisse zu protokollieren, die ausgenützt**

werden können, um einen nichtautorisierten Informationsfluß durch Ausnützung eines verdeckten Kanals zu erzeugen.

Wiederaufbereitung

A.56 Alle Speicherobjekte, die dem EVG wieder zur Verfügung gestellt werden, müssen vor einer Wiederverwendung durch andere Benutzer so aufbereitet werden, daß keine Rückschlüsse auf ihren früheren Inhalt möglich sind.

Beispiel: Funktionalitätsklasse F-B3

Zielsetzung

A.57 Die Beispielklasse F-B3 ist von den Funktionalitätsanforderungen der US-TCSEC-Klassen B3 und A1 abgeleitet. Zusätzlich zu den Funktionen der Klasse F-B2 werden Funktionen zur Unterstützung bestimmter Sicherheits-Administrationsrollen aufgenommen; außerdem wird die Protokollauswertung erweitert um eine Anzeige sicherheitsrelevanter Ereignisse.

Obligatorische Mechanismen

A.58 Diese Klasse verlangt, daß die Zugriffskontrolle durch einen einzigen "ReferenzValidierungsmechanismus" realisiert wird, der das "Referenz-Monitor-Konzept" erfüllt, d.h. der Mechanismus ist sicher gegen Veränderungen, immer eingeschaltet und so klein (ausreichend einfach), daß er Analysen und Tests unterzogen werden kann, deren Vollständigkeit garantiert werden kann.

Identifikation und Authentisierung

A.59 Der EVG muß Benutzer eindeutig identifizieren und authentisieren. Diese Identifikation und Authentisierung muß vor jeder anderen Interaktion des EVG mit dem Benutzer erfolgen. Weitere Interaktionen dürfen nur nach der erfolgreichen Identifikation und Authentisierung möglich sein. Die Authentisierungsinformationen müssen so gespeichert sein, daß nur autorisierte Benutzer darauf Zugriff haben. Identifikation und Authentisierung müssen über einen vertrauenswürdigen Pfad zwischen Benutzer und EVG abgewickelt werden, initiiert durch den Benutzer **oder den EVG.** Bei jeder Interaktion muß der EVG die Identität des Benutzers feststellen können.

Zugriffskontrolle

A.60 Der EVG muß in der Lage sein, Zugriffsrechte von jedem Benutzer auf Objekte, die der Rechteverwaltung unterliegen, zu unterscheiden und zu verwalten. Dies geschieht auf der Basis eines einzelnen Benutzers oder der Zugehörigkeit zu einer Benutzergruppe oder beidem. Es muß möglich sein, die Zugriffsrechte zur Unterstützung von Rollen in Gruppen zusammenzufassen. Mindestens die Rollen des EVG-Bedieners und -Systemverwalters müssen definierbar sein. **Die Rollen von Bediener, EVG-Systemverwalter und EVG-Sicherheitsbeauftragtem sind zu trennen.** Es muß möglich sein, Benutzern bzw. Benutzergruppen den Zugriff auf ein Objekt ganz zu verwehren. Daneben muß es ebenfalls möglich sein, den Zugriff eines Benutzers auf ein Objekt auf nicht-modifizierende Operationen einzuschränken. Es muß möglich sein, für jeden Benutzer einzeln die Zugriffsrechte bzgl. eines Objektes

zu erteilen. Keine Person, außer einem autorisierten Benutzer, darf die Möglichkeit haben, Rechte bzgl. eines Objektes zu vergeben oder zu entziehen.

A.61 **Für jedes der Rechteverwaltung unterliegende Objekt muß es möglich sein, eine Liste von Benutzern sowie eine Liste von Benutzergruppen unter Angabe ihrer jeweiligen Zugriffsrechte zu diesem Objekt anzugeben. Daneben muß es für jedes solche Objekt ebenfalls möglich sein, ein Verzeichnis von Benutzern sowie eine Liste von Benutzergruppen anzugeben, denen der Zugriff zu diesem Objekt verweigert ist.** Die Rechteverwaltung muß die Weitergabe von Zugriffsrechten kontrollieren. Ebenso darf das Einbringen neuer Benutzer, das Löschen von Benutzern sowie das zeitweilige Sperren aller Rechte eines Benutzers nur durch autorisierte Benutzer möglich sein.

A.62 Daneben muß der EVG alle Subjekte und Objekte (z.B. Prozesse, Dateien, Speichersegmente, Geräte) mit Attributen versehen. Der Wert dieser Attribute muß dabei als Grundlage für obligatorische Zugriffsrechte dienen. Es muß durch Regeln festgelegt werden, welche Kombination der Attributwerte von Subjekt und Objekt für ein Subjekt nötig ist, um Zugriff auf dieses Objekt zu erhalten.

A.63 Beim Export eines Objekts müssen die Attribute so mitexportiert werden, daß der Empfänger ihren Wert eindeutig rekonstruieren kann.

A.64 Die obligatorischen Zugriffsrechte müssen so gestaltet sein, daß der folgende Sonderfall realisiert werden kann:

Das Attribut besteht aus zwei Teilen. Der erste Teil besitzt hierarchisch geordnete Werte, der zweite stellt eine Menge dar. (Im Amtsbereich enthält der erste Teil Einstufungen, z.B. offen, vertraulich, geheim, streng geheim. Der zweite Teil enthält Kategorien.)

Ein Attribut A dominiert Attribut B genau dann, wenn:

Teil 1 von A hierarchisch größer oder gleich Teil 1 von B ist
und Teil 2 von B eine echte Teilmenge von oder gleich Teil 2 von A ist.

A.65 Die folgenden Regeln müssen durchgesetzt werden:

a) Lesender Zugriff eines Subjekts auf ein Objekt ist nur gestattet, wenn das Attribut des Subjekts das des Objekts dominiert.

b) Schreibender Zugriff eines Subjekts auf ein Objekt ist nur gestattet, wenn das Attribut des Objekts das des Subjekts dominiert.

A.66 Die Attribute eines Subjekts, das für einen Benutzer aktiv wird, werden dominiert durch die Ermächtigung und Autorisierung dieses Benutzers, wie sie zum Zeitpunkt der Identifikation und Authentisierung festgestellt wurde. Wenn importierte Daten

keine Attribute besitzen, muß ein autorisierter Benutzer in der Lage sein, diesen Daten Attribute zuzuordnen.

A.67 Exportkanäle müssen als einstufig oder mehrstufig identifizierbar sein. Über einen als einstufig gekennzeichneten Kanal dürfen nur Daten gesendet oder empfangen werden, wenn die Attribute dieser Daten mit einem vorab definierten Attribut übereinstimmen. Daten, die an einen einstufigen Kanal gesendet oder von einem einstufigen Kanal empfangen werden, müssen mit einem entsprechenden Attribut verbunden werden, wenn es einem autorisierten Benutzer nicht möglich ist, das Attribut des Kanals untäuschbar festzulegen. In diesem Fall wird das Attribut der Daten implizit durch das Attribut des Kanals festgelegt.

A.68 Bei mehrstufigen Kanälen muß durch das Übertragungsprotokoll sichergestellt sein, daß die Empfängerseite alle empfangenen Daten und Attribute vollständig und eindeutig rekonstruieren und dabei die Attribute den Daten eindeutig zuordnen kann. Für mehrstufige Kanäle muß es möglich sein, den maximalen und minimalen Attributwert anzugeben. Es dürfen keine Daten an einen mehrstufigen Kanal gesendet werden, wenn nicht das Attribut der Daten über das Minimalattribut des Kanals dominiert und seinerseits durch das Maximalattribut des Kanals dominiert wird.

A.69 Nichtautorisierten Benutzern muß es unmöglich sein, die sicherheitsrelevanten Attribute eines Kanals zu ändern. Eine Änderung dieser Attribute muß in expliziter Form erfolgen.

A.70 Der EVG muß menschenlesbare Ausgaben mit Attributwerten kennzeichnen. Die Werte der Attribute leiten sich aus den im EVG formulierten Regeln ab. Autorisierte Benutzer müssen in der Lage sein, den zu druckenden Namen jedes einzelnen Attributwerts zu spezifizieren.

A.71 Jede Änderung der Sicherheitsstufe, die einem Benutzer während einer laufenden interaktiven Sitzung zugeordnet ist, muß diesem Benutzer sofort angezeigt werden. Der Benutzer muß jederzeit die Möglichkeit haben, sich alle Attribute des Subjekts anzeigen zu lassen.

A.72 Bei jedem Zugriffsversuch von Benutzern bzw. Benutzergruppen auf Objekte, die der Rechteverwaltung unterliegen, hat der EVG die Berechtigung der Anforderung zu überprüfen. Unberechtigte Zugriffsversuche müssen abgewiesen werden. Die Werte der Attribute müssen als Grundlage für Entscheidungen bezüglich einer obligatorischen Zugriffskontrolle dienen. Die Regeln müssen eindeutig festlegen, wann ein Subjekt Zugriff auf ein derart geschütztes Objekt hat. Falls für ein Objekt zusätzlich noch benutzerbestimmbare Zugriffsrechte bestehen, darf ein Zugriff nur zugelassen werden, wenn sowohl die benutzerbestimmbaren als auch die obligatorischen Zugriffsrechte diesen Zugriff gestatten.

A.73 Es darf keine bekannten Speicher- und **zeitmodulierten** Kanäle geben, die Informationen zwischen Prozessen ohne Prüfung von Zugriffsrechten (d.h. verdeckt) übertragen können und die außerdem eine nichtakzeptabel hohe Bandbreite haben (festgestellt durch aktuelle Messung oder ingenieurmäßige Abschätzung). (Bezüglich

der Einschätzung von "Akzeptierbarkeit": Siehe auch den Abschnitt zu Covert channel Guidelines in den TCSEC [TCSEC]).

Beweissicherung

A.74 Der EVG muß eine Protokollierungskomponente enthalten, die in der Lage ist, jedes der folgenden Ereignisse mit den angegebenen Daten zu protokollieren:

a) Benutzung des Identifikations- und Authentisierungsmechanismus:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id., die angegeben wurde; Kennung des Gerätes, an dem der Identifikations- und Authentisierungsmechanismus benutzt wurde (z.B. Terminal-Id.); Erfolg bzw. Mißerfolg des Versuchs; Autorisierung des Benutzers.

b) Versuchter Zugriff auf ein der Rechteverwaltung unterliegendes Objekt:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Name des Objekts; Art des versuchten Zugriffs; Erfolg bzw. Mißerfolg des Versuchs; Attribut des Objekts.

c) Anlegen bzw. Löschen eines der Rechteverwaltung unterliegenden Objekts:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Name des Objektes; Art der Aktion; Attribut des Objekts.

d) Aktionen von autorisierten Benutzern, die die Sicherheit des EVG betreffen:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Art der Aktion; Name und Attribut des Objektes, auf das sich die Aktion bezog (Solche Aktionen sind z.B. das Einbringen oder Löschen (Sperren) von Benutzern; Einbringen oder Entfernen von Datenträgern; Starten bzw. Stoppen des EVG; Zuordnung eines Attributs; Änderung der Attribute, Kennzeichnungen oder Klassifikation eines Kanals).

A.75 Der Zugriff auf Protokollinformation darf nur dazu autorisierten Benutzern möglich sein. Es muß möglich sein, die Beweissicherung auf einen oder mehrere Benutzer zu beschränken. Werkzeuge zur Auswertung und Verwaltung von Protokolldaten müssen vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, selektiv die Aktionen eines oder mehrerer Benutzer zu identifizieren.

Protokollauswertung

A.76 Es müssen Werkzeuge zur Überprüfung der Protokolldateien zu Revisionszwecken vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, selektiv die Aktionen eines oder mehrerer Benutzer zu identifizieren. Zusätzlich muß der EVG in der Lage sein, bekannte Ereignisse zu protokollieren, die ausgenützt werden können, um einen nichtautorisierten Informationsfluß durch Ausnützung eines verdeckten Kanals zu erzeugen.

A.77 **Daneben muß es einen Mechanismus zur Überwachung von Ereignissen geben, die entweder besonders sicherheitsrelevant sind oder aufgrund der Häufigkeit ihres Auftretens eine kritische Bedrohung der Sicherheit des EVG werden könnten. Dieser Mechanismus muß in der Lage sein, einen speziellen Benutzer bzw. einen Benutzer mit einer speziellen Rolle unverzüglich über das Auftreten solcher Ereignisse zu informieren. Dieser Mechanismus muß daneben auch in der Lage sein, in solchen Fällen selbst Maßnahmen in die Wege zu leiten, durch welche ein weiteres Auftreten solcher Ereignisse unterbunden wird.**

Wiederaufbereitung

A.78 Alle Speicherobjekte, die dem EVG wieder zur Verfügung gestellt werden, müssen vor einer Wiederverwendung durch andere Benutzer so aufbereitet werden, daß keine Rückschlüsse auf ihren früheren Inhalt möglich sind.

Beispiel: Funktionalitätsklasse F-IN

Zielsetzung

A.79 Die Beispiel-Funktionalitätsklasse F-IN ist für EVG mit hohen Integritäts-anforderungen an Daten und Programme vorgesehen. Solche Anforderungen sind beispielsweise bei Datenbank-EVG von Bedeutung.

Identifikation und Authentisierung

A.80 Der EVG muß Benutzer eindeutig identifizieren und authentisieren. Diese Identifikation und Authentisierung muß vor jeder anderen Interaktion zwischen EVG und Benutzer erfolgen. Weitere Interaktionen dürfen nur nach der erfolgreichen Identifikation und Authentisierung möglich sein. Die Authentisierungsinformationen müssen so gespeichert sein, daß nur autorisierte Benutzer sie prüfen oder ändern können. Bei jeder Interaktion muß der EVG die Identität des Benutzers feststellen können.

Rechteverwaltung

A.81 Der EVG muß Zugriffsrechte von Benutzern, Rollen und Prozessen zu speziell adressierten Objekten unterscheiden und verwalten können. (Der Begriff "Rollen" bezeichnet Benutzer mit besonderen Attributen.) Dabei muß es möglich sein, den Zugriff von Benutzern auf diese Objekte so einzuschränken, daß dieser Zugriff nur über speziell festgelegte Prozesse möglich ist. Ferner muß es möglich sein, Objekte einem vordefinierten Typ zuzuordnen. Ebenso muß es möglich sein, für jeden Typ von Objekten festzulegen, welche Benutzer, Rollen oder Prozesse welche Art von Zugriffsrechten auf diese Objekte besitzen können. Dadurch sollte es möglich sein, den Zugriff von Benutzern auf Objekte eines bestimmten Typs so einzuschränken, daß dieser Zugriff nur über festgelegte Prozesse möglich ist. Nur speziell autorisierten Benutzern darf es möglich sein, neue Typen zu definieren bzw. Zugriffsrechte zu Typen zu vergeben oder zu entziehen. Diese Aktionen müssen explizit von diesem speziellen Benutzer initiiert werden. Bei diesen Aktionen müssen alle Kommunikationen zwischen EVG und Benutzer über einen vertrauenswürdigen Pfad ablaufen.

A.82 Mindestens folgende Zugriffsrechte müssen vorliegen: Lesen, Schreiben, Einfügen, Löschen, Umbenennen (für alle Objekte), Ausführen, Löschen, Umbenennen (für ausführbare Objekte), Anlegen von Objekten eines bestimmten Typs, Löschen von Objekten eines bestimmten Typs.

A.83 Bei jedem Zugriffsversuch einzelner Benutzer oder Benutzergruppen auf Objekte, die der Rechteverwaltung unterliegen, muß der EVG die Berechtigung des Zugriffs überprüfen. Unberechtigte Zugriffsversuche müssen abgewiesen werden.

Beweissicherung

A.84 Der EVG muß eine Protokollierungskomponente enthalten, die in der Lage ist, folgende Ereignisse mit den angegebenen Daten zu protokollieren:

a) Benutzung des Identifikations- und Authentisierungsmechanismus:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id., die angegeben wurde; Kennung des Gerätes, an dem der Identifikations- und Authentisierungsmechanismus benutzt wurde (z.B. Terminal-Id.); Erfolg bzw. Mißerfolg des Versuchs.

b) Versuchter Zugriff auf ein der Rechteverwaltung unterliegendes Objekt:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Name des Objekts; Art des versuchten Zugriffs; Erfolg bzw. Mißerfolg des Versuchs.

c) Anlegen bzw. Löschen eines der Rechteverwaltung unterliegenden Objekts:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Name des Objektes; Art der Aktion.

d) Aktionen von autorisierten Benutzern, die die Sicherheit des EVG betreffen:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Art der Aktion; Name und Attribut des Objektes, auf das sich die Aktion bezog (Solche Aktionen sind z.B. das Einbringen oder Löschen (Sperren) von Benutzern; Einbringen oder Entfernen von Datenträgern; Starten bzw. Stoppen des EVG).

e) Definition oder Löschen von Typen:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Art der Aktion; Name des Typs.

f) Zuordnung eines Typs zu einem Objekt:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Name des Objekts; Name des Typs.

g) Erteilung oder Entzug von Zugriffsrechten für ein Objekt oder einen Objekttyp:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id.; Art der Aktion; Art des Zugriffsrechts; Name des Subjekts; Name des Objekts oder Name des Objekttyps.

A.85 Der Zugriff auf Protokollinformationen darf nur dazu autorisierten Benutzern möglich sein. Es muß möglich sein, die Aktionen eines oder mehrerer Benutzer selektiv zu protokollieren. Werkzeuge zur Auswertung und Verwaltung von Protokolldaten müssen vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, selektiv die Aktionen eines oder mehrerer Benutzer zu identifizieren. Der Aufbau der Protokolleinträge muß vollständig beschrieben werden.

Protokollauswertung

A.86 Es müssen Werkzeuge zur Überprüfung der Protokolldateien zu Revisionszwecken vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, die Aktionen eines oder mehrerer Benutzer selektiv zu identifizieren.

Beispiel: Funktionalitätsklasse F-AV

Zielsetzung

A.87 Die Beispiel-Funktionalitätsklasse F-AV stellt hohe Anforderungen an die Verfügbarkeit eines kompletten EVG bzw. spezieller Funktionen eines EVG. Solche Anforderungen sind z.B. bei Prozeßsteuerungs-EVG von Bedeutung.

Zuverlässigkeit der Dienstleistungen

A.88 Der EVG muß in der Lage sein, den Ausfall bestimmter einzelner Hardware-Komponenten (z.B. einer Platte oder eines einzelnen Prozessors in einem Mehrprozessor-EVG) so zu überbrücken, daß alle fortlaufend benötigten Funktionen auch in dem Rest-EVG kontinuierlich zur Verfügung stehen. Nach der Reparatur der ausgefallenen Komponente muß diese so wieder in den EVG integriert werden können, daß ein kontinuierlicher Betrieb der fortlaufend benötigten Funktionen gewährleistet ist. Nach der Integration muß der EVG wieder seinen ursprünglichen Grad der Ausfallsicherheit erreicht haben. Für die Dauer eines solchen Integrationsprozesses sind Maximalzeiten anzugeben.

A.89 Der EVG muß unabhängig von seiner momentanen Auslastung für bestimmte Aktionen eine maximale Reaktionszeit gewährleisten. Daneben muß für festgelegte Aktionen die Verklemmungsfreiheit (deadlock) des EVG gewährleistet sein.

Beispiel: Funktionalitätsklasse F-DI

Zielsetzung

A.90 Die Beispiel-Funktionalitätsklasse F-DI stellt hohe Anforderungen an die Sicherung der Integrität von Daten bei der Datenübertragung.

Identifikation und Authentisierung

A.91 Der EVG muß Benutzer eindeutig identifizieren und authentisieren. Diese Identifikation und Authentisierung muß vor jeder anderen Interaktion zwischen dem EVG und Benutzer erfolgen. Weitere Interaktionen dürfen nur nach der erfolgreichen Identifikation und Authentisierung möglich sein. Die Authentisierungsinformationen müssen so gespeichert sein, daß nur autorisierte Benutzer sie prüfen oder ändern können. Bei jeder Interaktion muß der EVG die Identität des Benutzers feststellen können.

A.92 Vor der Herstellung einer Verbindung muß der Kommunikationspartner (Rechner, Prozess oder Benutzer) eindeutig identifiziert und authentisiert werden. Erst nach der erfolgreichen Identifikation und Authentisierung darf eine Übertragung von Nutzdaten erfolgen. Beim Empfang von Daten muß deren Absender eindeutig identifiziert und authentisiert werden können. Alle Authentisierungsdaten müssen vor unbefugtem Zugriff und vor Fälschung geschützt sein.

Beweissicherung

A.93 Der EVG muß eine Protokollierungskomponente enthalten, die in der Lage ist, folgende Ereignisse mit den angegebenen Daten zu protokollieren:

a) Benutzung des Identifikations- und Authentisierungsmechanismus:

   Geforderte Daten: Datum; Uhrzeit; Initiator der Identifikation und Authentisierung; Name des zu identifizierenden Subjekts; Erfolg bzw. Mißerfolg des Versuchs.

b) Identifizierte Fehler bei der Datenübertragung:

   Geforderte Daten: Datum; Uhrzeit; Kommunikationspartner der Datenübertragung; Art des Fehlers; Erfolg bzw. Mißerfolg des Korrekturversuchs.

c) Datenübertragung:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id. des Initiators; Name des Kommunikationspartners (Rechner, Prozess oder Benutzer); Parameter für die Herstellung der Verbindung (wenn dabei Unterschiede zu berücksichtigen sind).

A.94 Der Zugriff auf Protokollinformationen darf nur dazu autorisierten Benutzern möglich sein. Es muß möglich sein, die Aktionen eines oder mehrerer Benutzer selektiv zu protokollieren. Werkzeuge zur Auswertung und Verwaltung von Protokolldaten müssen vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, selektiv die Aktionen eines oder mehrerer Benutzer zu identifizieren. Der Aufbau der Beweissicherungseinträge muß vollständig beschrieben werden.

Protokollauswertung

A.95 Es müssen Werkzeuge zur Überprüfung der Protokolldateien zu Revisionszwecken vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, die Aktionen eines oder mehrerer Benutzer selektiv zu identifizieren.

Datenübertragung

Datenintegrität

A.96 Bei der Datenübertragung müssen Methoden zur Fehlererkennung und Fehlerbehebung eingesetzt werden. Diese Mechanismen sind so zu gestalten, daß absichtliche Manipulationen an den Adressfeldern und den Nutzdaten erkannt werden können. Daneben darf die bloße Kenntnis der eingesetzten Algorithmen ohne spezielle Zusatzkenntnisse nicht ausreichen, unerkannte Manipulationen an den obengenannten Daten vorzunehmen. Die hierzu benötigten Zusatzkenntnisse müssen derart geschützt sein, daß nur einige wenige, speziell autorisierte Benutzer Zugang dazu haben.

A.97 Des weiteren sind Mechanismen einzusetzen, die auch ein unbefugtes Wiedereinspielen von Daten zuverlässig als Fehler erkennen.

Beispiel: Funktionalitätsklasse F-DC

Zielsetzung

A.98 Die Beispiel-Funktionalitätsklasse F-DC ist für EVG vorgesehen, die hohe Anforderungen an die Geheimhaltung von Informationen bei der Datenübertragung stellen. In diese Klassen fallen beispielsweise Verschlüsselungsgeräte.

Datenübertragung

Vertraulichkeit der Daten

A.99 Der EVG muß über eine Vorrichtung verfügen, Nutzdaten vor einer Übertragung automatisch zu verschlüsseln und sie (empfängerseitig) automatisch zu entschlüsseln. Hierzu ist ein von einer autorisierten Prüfstelle zugelassener Algorithmus zu verwenden. Es ist sicherzustellen, daß die zur Entschlüsselung benötigten Parameterwerte (z.B. Schlüssel) in der Weise geschützt sind, daß kein Unbefugter Zugang zu diesen Daten besitzt.

Beispiel: Funktionalitätsklasse F-DX

Zielsetzung

A.100 Die Beispiel-Funktionalitätsklasse F-DX ist für vernetzte Systeme gedacht, die hohe Anforderungen an die Geheimhaltung und Integrität von Informationen bei der Datenübertragung stellen. Dies kann beispielsweise der Fall sein, wenn sensitive Daten über ungesicherte (z.B. öffentliche) Netze übertragen werden müssen.

Identifikation und Authentisierung

A.101 Der EVG muß Benutzer eindeutig identifizieren und authentisieren. Diese Identifikation und Authentisierung muß vor jeder anderen Interaktion zwischen EVG und Benutzer erfolgen. Weitere Interaktionen dürfen nur nach der erfolgreichen Identifikation und Authentisierung möglich sein. Die Authentisierungsinformationen müssen so abgespeichert sein, daß nur autorisierte Benutzer sie prüfen oder ändern können. Bei jeder Interaktion muß der EVG die Identität des Benutzers feststellen können.

A.102 Vor der Übertragung von Nutzerdaten muß der Kommunikationspartner (Rechner, Prozess oder Benutzer) eindeutig identifiziert und authentisiert sein. Erst nach der erfolgreichen Identifikation und Authentisierung darf eine Übertragung von Nutzdaten erfolgen. Beim Empfang von Daten muß deren Absender eindeutig identifiziert und authentisiert werden können. Alle Authentisierungsdaten müssen vor unbefugtem Zugriff und vor Fälschung geschützt sein.

Beweissicherung

A.103 Der EVG muß eine Protokollierungskomponente enthalten, die in der Lage ist, folgende Ereignisse mit den angegebenen Daten zu protokollieren:

a) Benutzung des Identifikations- und Authentisierungsmechanismus:

   Geforderte Daten: Datum; Uhrzeit; Initiator der Identifikation und Authentisierung; Name des zu identifizierenden Subjekts; Erfolg bzw. Mißerfolg des Versuchs.

b) Identifizierte Fehler bei der Datenübertragung:

   Geforderte Daten: Datum; Uhrzeit; Kommunikationspartner der Datenübertragung; Art des Fehlers; Erfolg bzw. Mißerfolg des Korrekturversuchs.

c) Herstellen der Verbindung:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id. des Initiators; Name des Kommunikationspartners (Rechner, Prozess oder Benutzer); Verbindungsparameter (wenn dabei Unterschiede zu berücksichtigen sind).

d) Spezielle Datenübertragungs-Transaktionen:

Geforderte Daten: Datum; Uhrzeit; Benutzer-Id. des sendenden Benutzers; Benutzer-Id. des Empfängers; übertragene Benutzer-Informationen; Datum und Uhrzeit des Empfangs.

A.104 Der Zugriff auf Protokollinformationen darf nur dazu autorisierten Benutzern möglich sein. Es muß möglich sein, die Aktionen eines oder mehrerer Benutzer selektiv zu protokollieren. Werkzeuge zur Auswertung und Verwaltung von Protokolldaten müssen vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, selektiv die Aktionen eines oder mehrerer Benutzer zu identifizieren. Der Aufbau der Protokolleinträge muß vollständig beschrieben werden.

Protokollauswertung

A.105 Es müssen Werkzeug zur Überprüfung der Protokolldateien zu Revisionszwecken vorhanden und dokumentiert sein. Diese Werkzeuge müssen es ermöglichen, die Aktionen eines oder mehrerer Benutzer selektiv zu identifizieren.

Datenübertragung

Zugriffskontrolle

A.106 Alle bereits übertragenen Informationen, die für eine nicht autorisierte Entschlüsselung verwendet werden können, müssen so geschützt werden, daß sie ausschließlich für Personen zugänglich sind, die einen Zugriff darauf für die Durchführung ihrer Arbeiten benötigen.

Vertraulichkeit der Daten

A.107 Der EVG muß die Möglichkeit einer Ende-zu-Ende-Verschlüsselung bieten, die eine Geheimhaltung im Hinblick auf den Empfänger über weite Teile des Übertragungsweges gewährleistet. Zusätzlich muß die Geheimhaltung des Übertragungsaufkommens auf speziellen Datenübertragungskanälen garantiert werden.

Datenintegrität

A.108 Der EVG muß so entworfen werden, daß unbefugte Manipulationen von Nutzdaten und Protokolldaten sowie ein unbefugtes Wiedereinspielen von Daten zuverlässig als Fehler erkannt werden.

ANHANG B - DIE CLAIMS-SPRACHE *)

EINLEITUNG

B.1 Im Zusammenhang mit den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik ist es hilfreich, ein Mittel zur Hand zu haben, mit dem Aussagen bezüglich der Sicherheitsfunktionen eines IT-Sicherheitproduktes in einer semiformalen Notation und dabei trotzdem mit natürlichen Sprachmitteln beschrieben werden können. Die in diesem Anhang definierte Claims-Sprache wurde zu diesem Zweck entwickelt.

B.2 Die Vorteile der Verwendung der Claims-Sprache bei der Beschreibung der Sicherheitsfunktionalität sind:

a) Sie bietet eine auf natürlicher Sprache basierende semiformalen Notation, die ohne spezielle Kenntnisse der Schreibweise oder Regeln gelesen werden kann,

b) sie zeigt die erforderliche Verbindung und Gruppierung von Postulaten auf,

c) sie reduziert das Maß der Mehrdeutigkeiten bei der Interpretation von Postulaten,

d) sie ermöglicht es, die Postulate bezüglich eines EVG in einer Weise auszudrücken, die dem Evaluationsprozess angepaßt ist.

B.3 Die Claims-Sprache ermöglicht eine kontrollierte Erweiterung der vordefinierten Notation zur Behandlung von Konzepten, für die keine geeigneten Elemente existieren. Innerhalb eines Claims-Dokumentes können auch in natürlicher Sprache Mechanismen und Annahmen beschrieben werden, falls kein formalerer Ansatz erforderlich ist. Die Claims-Sprache ist flexibel genug, um alle Postulate, die für einen bestimmten EVG zutreffen, zu definieren, ohne von den Regeln der Sprache abzuweichen; der Antragsteller einer Evaluation ist somit in keiner Weise gezwungen, seine Postulate an die Sprache anzupassen.

Übersicht

B.4 Mit Hilfe der Claims-Sprache werden Sicherheitsfunktionen dargestellt. Hierfür wird eine Sammlung von Regeln für die Erzeugung von Schablonen für Aktionssätze ausgedrückt, von denen jede den Rahmen für einen speziellen Aussage-Typ liefert. Jede Schablone für Aktionssätze wird dann mit einem Zielsatz aus einer Menge von Zielsätzen kombiniert, um ein Aussageschema zu erzeugen. Substantive und Satzteile, die für das Produkt, die Funktion und/oder den Anbieter spezifisch sind, werden dann in das Aussageschema eingesetzt, um auf diese Weise eine echte Aussage, z.B. ein Postulat, zu formulieren. Ein Beispiel für die Erzeugung einer Aussage ist in den Absätzen B.30 bis B.34 dieses Anhanges dargestellt.

*) Anm. d. Übers.: Der Begriff "claim" ist im hier gegebenen Zusammenhang nicht problemlos ins Deutsche übersetzbar. Deshalb wird in diesem Kapitel u.a. auch der englische Originalbegriff verwendet. Siehe hierzu auch Abschnitt 2.75

B.5 Als Teil eines Postulats ist es möglich, einen Bezug auf den das Postulat realisierenden Mechanismus mitaufzunehmen.

B.6 Es ist zulässig, die Verbindungsworte auszulassen oder zu ändern, die im Aussageschema verwendet wurden, um damit die sprachliche Verständlichkeit oder grammatikalische Exaktheit von Aussagen zu gewährleisten.

B.7 Beispiele für mögliche Änderungen sind:

a) Ersetzen des Singular durch den Plural und umgekehrt;

b) Einfügen von bestimmten oder unbestimmten Artikeln;

c) Ändern von Präpositionen.

B.8 In Fällen, in denen keine geeigneten Sätze vorliegen, ist es zulässig, neue Aktions- oder Zielsätze unter der Voraussetzung einzuführen, daß solche Sätze mit der Zertifizierungsstelle abgesprochen und von ihr genehmigt wurden.

B.9 Dokumente, die Claims-Formulierungen enthalten, müssen einem Standard-Format entsprechen, das in Paragraph B.38 bis B.40 dieses Anhangs niedergelegt ist. Die Postulate sind unter standardisierten Oberbegriffen zusammenzufassen, die auf den generischen Oberbegriffen für die Funktionalität basieren. Dies erleichtert das Verständnis und vereinfacht den Vergleich mit anderen EVG.

Warnungen

B.10 Bei der Formulierung von konfigurationsabhängigen Aussagen ist Vorsicht geboten. Es kann möglich sein, einen EVG so zu konfigurieren, daß Unsicherheiten entstehen (d.h., einige der Aussagen werden ungültig). Wenn dies der Fall ist, sind Einschränkungen zur Eliminierung solcher unsicheren Optionen und Kombinationen von Optionen als umgebungsrelevante Einschränkung anzugeben (siehe Paragraph B.41 und folgende in diesem Anhang).

B.11 Des weiteren sollte darauf geachtet werden, die Aussagen in einer angemessen detaillierten Form zu formulieren. Wenn eine vorgesehene Aussage augenscheinlich unter mehrere generische Oberbegriffe fällt oder mehr Substitutionen erfordert, als es mit der entsprechenden Schablone möglich ist, dann ist diese Aussage auf einer zu hohen Stufe angesiedelt und muß in eine Reihe einfacherer Aussagen aufgeteilt werden.

Schablonen für Aktionssätze

B.12 Schablonen für Aktionssätze sind aus dem unten angegebenen Rahmen zu erstellen. Worte oder Sätze in der Schablone, die kursiv gesetzt sind, sind durch die auf die Aussage bezogenen Fakten zu ersetzen, wobei [] wahlfreie Teile und <> die Auswahl einer Option aus der entsprechenden, nachfolgenden Optionsliste bedeuten:

Der vorliegende *EVG* [<Indikator>] <Verb> <Aktion> ... [<Zeit>] [unter Verwendung des in Paragraph *n* definierten Mechanismus]

<Indikator> kann sein:

enthält eine *Funktion*, die
oder muß in einer Umgebung verwendet werden, die

<Verb> kann sein:

wird
oder wird nicht
oder kann so konfiguriert werden, daß
oder kann so konfiguriert werden, daß nicht
oder kann nicht so konfiguriert werden, daß

<Aktion> kann sein:

festlegen
oder erkennen
oder kontrollieren
oder erlauben
oder verhindern
oder gewährleisten
oder protokollieren in *Objekt*

<Zeit> kann sein:

vor *sicherheitsrelevantem Ereignis*
oder nach *sicherheitsrelevantem Ereignis*

B.13 Die Umgebungsoption <Indikator> wird nur in den Fällen zur Definition umgebungsrelevanter Einschränkung verwendet, in denen hohe Präzision gefordert ist.

B.14 Wo Details spezifischer Mechanismen Bestandteil der Sicherheitsvorgaben sind, müssen sie als Teil des Claims-Dokuments definiert werden. Dies wird durch Bezug auf einen

Paragraph erreicht, der die Mechanismus-Spezifikation enthält. Wenn ein solcher Bezug nicht vorhanden ist, sind die Einzelheiten der Mechanismen kein Bestandteil der Sicherheitsvorgaben und werden als urheberrechtlich geschützte Information behandelt. Die Funktionsoption <Indikator> kann wahlfrei eingesetzt werden. Damit wird der bestimmte Produktmechanismus benannt, der eine bestimmte Aussage realisiert. Dieser Name wird lediglich erklärungshalber aufgenommen.

B.15 Einige Beispiele für Schablonen für Aktionssätze:

Dieses Produkt stellt sicher ...

Dieses Produkt enthält ein Protokollauswerte-Dienstprogramm, das feststellt...

Dieses Produkt kann so konfiguriert werden, daß es möglich ist, ...

Dieses Produkt muß in einer Umgebung eingesetzt werden, die ... verhindert

Diese Zusatzplatine sammelt als Protokollinformation ...

Dieses Produkt verhindert vor Beendigung des sicheren Anlaufs, daß ...

Zielsätze

B.16 Nachfolgend die zugelassene Menge der Zielsätze, wobei [] wahlfreie Teile der Sätze angeben:

1 ... *Protokoll-Informationen* bezüglich *sicherheitsrelevanter Ereignisse*

2 ... die Identität eines aufgerufenen *Prozesses*

3 ... die Identität des *{Benutzer, Prozeß},* der einen *Prozeß* aufruft

4 ... die Identität des *{Benutzer, Prozeß},* der einen *Zugriffstyp* zu einem *Objekt* verlangt

5 ... die Identität eines ausgeführten *Prozesses*

6 ... die Zurückweisung eines aufgerufenen *Prozesses*

7 ... die Identität eines *Objekts*, zu welchem ein *Zugriffstyp* verlangt wurde

8 ... die Identität eines *Objekts*, zu welchem ein *Zugriffstyp* gewährt wurde

9 ... die Identität eines *Objekts*, zu welchem ein *Zugriffstyp* verwehrt wurde

10 ... die *Zugriffseinstellung* eines *Benutzers*

11 ... die *Zugriffseinstellung* eines *Prozesses*

12 ... die *Zugriffseinstellung* eines *{Benutzer, Prozeß}*

13 ... die *Zugriffseinstellung* eines *Objekts*

14 ... der *Zugriffstyp*, der einem *{Benutzer, Prozeß}* bezüglich eines *Objekts* gewährt wurde

15 ... der *Zugriffstyp* von *{Benutzer, Prozeß}* bezüglich eines *Objektes*

16 ... die Handlungen, die durch einen *{Benutzer, Prozeß}* bezüglich eines *Objekts* ausgeführt wurden

17 ... die *Faktoren*, die die *Zugriffseinstellung* eines *Benutzers* berühren

18 ... die *Faktoren*, die die *Zugriffseinstellung* eines *Prozesses* berühren

19 ... die *Faktoren*, die die *Zugriffseinstellung* eines *{Benutzer, Prozeß}* berühren

20 ... die *Faktoren*, die die *Zugriffseinstellung* eines *Objekts* berühren

21 ... das Löschen von Informationen aus einem *Objekt*

22 ... die *Sicherheitsattribute* eines *Objekts*

23 ... die Korrektheit der *Sicherheitsattribute* eines *Objekts*

24 ... die *Sicherheitsattribute* eines *Objekts*, das aus der Kombination von *Objekten* gebildet wird

25 ... die *Sicherheitsattribute* einer Anzahl von *Objekten*, die durch die Aufteilung eines einzelnen *Objekts* gebildet werden

26 ... die Gewährung eines *Zugriffstyp* zu einem *Objekt* kann nicht zur Verklemmung führen, wenn *{Benutzer, Prozesse}* den *Zugriffstyp* zu *Objekten* benutzen

27 ... die Benutzung eines *Zugriffstyp*s durch *{Benutzer, Prozesse}* zu einem *Objekt*, die zur Verklemmung geführt hat

28 ... die Gewährung eines *Zugriffstyp* zu einem *Objekt* kann nicht zu einem "Livelock" führen, wenn *{Benutzer, Prozesse}* den *Zugriffstyp* zu *Objekten* benutzen

29 ... die Benutzung eines *Zugriffstyps* durch *{Benutzer, Prozesse}* zu einem *Objekt*, die zu einem "Livelock "geführt hat

30 ... *Sicherheitsattribut* des *Objekts* ist identisch mit dem des *Objekts*

31 ... *Aussage*, soll [nicht] zeitkritisch werden

32 ... *Aussage*, soll [nicht] beschleunigt oder verzögert werden

33 ... *Aussage*, soll [nicht] zeitabhängig werden

34 ... *Aussage*, soll [nicht] umgangen werden

35 ... *Aussage*, soll [nicht] deaktiviert werden

36 ... *Aussage*, soll [nicht] korrumpiert werden

Substitutionen

B.17 Substitutionen sind an den folgenden *(in den obigen Schablonen für Aktionssätze und Zielsätze kursiv gedruckten)* Substantiven/Sätzen vorzunehmen:

Zugriffseinstellung; Zugriffstyp; Protokoll-Informationen; Aussage; Faktor; Funktion; n; Objekt; Produkt; Prozeß; Sicherheitsattribut; sicherheitsrelevantes Ereignis; Benutzer; {Benutzer, Prozeß}

B.18 Alle Substitutionen sind in natürlicher Sprache entweder in einem separaten Abschnitt des Claims-Dokuments (s. Paragraph B.39 dieses Anhangs) oder unmittelbar im Anschluß an die Aussage, in welcher die Substitution vorgenommen wurde, zu erklären.

B.19 Einige Beispiele von möglichen Substitutionen:

Zugriffseinstellung	ersetzt durch	Schreib/Lesezugriff auf I/O-Kanäle
Zugriffstyp	ersetzt durch	Leseerlaubnis
Zugriffstyp	ersetzt durch	Lese/Schreib/Löscherlaubnis
Protokoll-Information	ersetzt durch	Datum und Uhrzeit
Protokoll-Information	ersetzt durch	Terminalnummer
Aussage	ersetzt durch	(Querverweis auf andere Aussage)
Faktoren	ersetzt durch	Anzahl ungültiger Antworten
Funktion	ersetzt durch	Passwortsystem
n	ersetzt durch	(Paragraphennummer)
Objekt	ersetzt durch	Datei
Objekt	ersetzt durch	Betriebsmittel-Kontrollblock

Objekt	ersetzt durch	Festplattenspeicher (d.h. Objekttyp)
EVG	ersetzt durch	Betriebssystem
EVG	ersetzt durch	PC-Sicherheitsplatine
Prozeß	ersetzt durch	unprivilegierte Task
Sicherheitsattribut	ersetzt durch	Datenintegrität
Sicherheitsattribut	ersetzt durch	tatsächlicher Zielort
Sicherheitsattribut	ersetzt durch	erkennbare Quelle
Sicherheitsrelevantes Ereignis	ersetzt durch	versuchte Verletzung von Privilegien
Sicherheitsrelevantes Ereignis	ersetzt durch	Benutzerabmeldung
Sicherheitsrelevantes Ereignis	ersetzt durch	Änderung der Sicherheitsstufe
Benutzer	ersetzt durch	Datentypistin
Benutzer	ersetzt durch	Sicherheitsadministrator
{Benutzer, Prozeß}	ersetzt durch	Job (d.h. Implizierung eines beliebigen Benutzers)

B.20 Teile der Aktionssätze und Zielsätze stehen in eckigen Klammern []; hierbei handelt es sich um wahlfreie Worte oder Sätze, die den Aussagen des Anbieters falls notwendig beigefügt oder weggelassen werden können.

B.21 Die meisten Substitutionen von Substantiven und Sätzen sind problemlos möglich. Es bestehen allerdings einige Konventionen, die nachstehend erläutert werden.

B.22 Die Definition einer Zugriffseinstellung hängt davon ab, worauf sich der Begriff bezieht:

a) auf ein Objekt; in diesem Fall ist es die Liste der Benutzer, Prozesse und {Benutzer, Prozesse}, die in der Lage sind, ein Objekt zu benützen, jeweils mit einem dazugehörigen Zugriffstyp;

b) auf einen Benutzer oder Prozeß oder {Benutzer, Prozesse}: in diesem Fall ist es die Liste der Objekte, die einem Benutzer, Prozeß oder {Benutzer, Prozesse} zur Verfügung stehen, jeweils mit einem dazugehörigen Zugriffstyp.

B.23 Die Zugriffseinstellung ist also ein (nominelles) Verzeichnis aller Objekte, auf die ein Benutzer wie und unter Verwendung welcher Prozesse zugreifen kann, oder ein (nominelles) Verzeichnis aller Benutzer, die auf ein Objekt wie und unter Verwendung welchen Prozesses zugreifen können.

B.24 Als Zugriffstyp bezeichnet man die vom Hersteller festgelegten, unterschiedlichen Möglichkeiten der Verwendung eines Objekts. Typische Beispiele hierfür sind *erstellen, lesen, schreiben, löschen, ausführen* oder eine Kombination hieraus oder *kein Zugriff*.

B.25 Als spezifisches Beispiel ließe sich folgender Wertebereich definieren:

a) "Ändern" erlaubt die Aktualisierung eines Datensatzes, nicht jedoch das Hinzufügen neuer Datensätze in eine Datei.

b) "Erstellen" erlaubt das Hinzufügen neuer Datensätze in eine Datei, nicht jedoch die Veränderung der bereits darin enthaltenen Datensätze.

c) "Löschen" erlaubt Löschen von Datensätzen aus der Datei.

d) "Ausführen" erlaubt es, die Datei in den Speicher zu laden und als ablauffähiges Programm vorzusehen.

e) "Lesen" ermöglicht das Kopieren von Datensätzen in den Arbeitsspeicher.

B.26 Viele Objekte werden identische Sicherheitsattribute haben. Wenn eine Aussage also für alle Objekte eines bestimmten Typs gilt, so ist es besser, die Substitution anhand des Objekttyps auszudrücken, anstatt alle möglichen Objekte dieses Typs aufzulisten.

Mechanismen

B.27 Als Teil einer Aussage ist es möglich, eine Beschreibung des zur Realisierung dieser Aussage verwendeten Mechanismus mitaufzunehmen. Dies erfolgt durch die Option "verwenden" der Schablone für Aktionssätze. Dabei wird auf einen Paragraphen des Claims-Dokumentes Bezug genommen, der den verwendeten Mechanismus spezifiziert und/oder erklärt. In der Evaluation wird dann die Bestätigung enthalten sein, daß der angegebene Mechanismus auch der verwendete Mechanismus ist.

B.28 Zur Definition oder Beschreibung des Mechanismus kann jede geeignete Methode verwendet werden, vorausgesetzt, daß die Erklärung für die Evaluation ausreichend ist, um mit dem der angestrebten Evaluationsstufe entsprechenden Vertrauen festzulegen, ob:

a) der postulierte Mechanismus in dem Produkt vorhanden ist,

b) sein Betriebsverhalten mit der Spezifikation übereinstimmt,

c) es sich tatsächlich um den Mechanismus handelt, der zur Realisierung der Aussage verwendet wird.

B.29 In vielen Fällen wird es einfacher und anschaulicher sein, einen Mechanismus durch Verweis auf einen veröffentlichten Standard zu definieren oder eine Tabelle der Eingaben und der entsprechenden Ergebnisse anzugeben, anstatt Details über den verwendeten Algorithmus in natürlicher Sprache oder in Form einer Spezifikation oder eines Programms anzugeben.

Beispiel

B.30 Mit den angegebenen Regeln kann zum Beispiel die folgende Schablone für Aktionssätze erzeugt werden:

Dieses *EVG* stellt fest ...

wobei das kursiv gesetzte Wort durch einen spezifischen Begriff ersetzt werden kann.

B.31 Desgleichen kann ein Zielsatz wie folgt gewählt werden:

... die Identität eines *Objektes*, zu dem *Zugriffstyp* verlangt wurde.

B.32 Zusammengefaßt ergibt dies folgendes:

Dieses *EVG* stellt die Identität eines *Objektes* fest, zu dem *Zugriffstyp* verlangt wurde

wobei z.B. die folgenden Substitutionen möglich sind:

Zusatz-Sicherheitsplatine	ersetzt	*EVG*
jede Datei	ersetzt	*Objekt*
Schreib- oder Leseerlaubnis	ersetzt	*Zugriffstyp*

B.33 Die vollständige Aussage könnte also lauten:

Diese Zusatz-Sicherheitsplatine stellt die Identität jeder Datei fest, zu der Schreib- oder Leseerlaubnis verlangt wurde.

B.34 Dieses Beispiel ist augenscheinlich sehr künstlich. In der Praxis werden für EVG sehr spezifische Aussagen geltend gemacht, die sich oft auf eine spezielle reale oder angenommene Umgebung beziehen.

Struktur des Claims-Dokumentes

Verwendung der generischen Oberbegriffe für die Funktionalität

B.35 Aussagen zur Funktionalität sind unter den in Kapitel 2 beschriebenen generischen Oberbegriffen zusammenzufassen. Nicht alle EVG werden unter allen Oberbegriffen Aussagen machen; wo keine Aussagen gemacht werden sollen, muß dies unter dem entsprechenden Oberbegriff angegeben werden. Für jedes Ereignis oder jede Aktion, die nicht vorkommen dürfen, müssen Aussagen vorhanden sein.

B.36 Tabelle B.1 zeigt Zielsätze, die des öfteren unter speziellen generischen Oberbegriffen erscheinen werden. Diese Tabelle ist lediglich eine allgemeine Richtlinie; die

Flexibilität der Claims-Sprache bedeutet auch, daß andere Zielsätze häufig ebenfalls geeignet sein werden.

B.37 Tabelle B.2 zeigt den Querverweis zwischen Zielsätzen und den in ihnen möglichen Substitutionen.

Format des Claims-Dokumentes

B.38 Die in der Claims-Sprache verfaßten Sicherheitsvorgaben sind wie folgt aufzubauen:

a) die Sicherheitsziele zusammen mit den Einschränkungen und Annahmen bezüglich der realen oder angenommenen Einsatzumgebung des EVG, in Form einer Produkt-Beschreibung (oder - im Falle eines Systems - einer System-Sicherheitspolitik);

b) eine informelle Spezifikation der Postulate in natürlicher Sprache, oder ein Verweis auf ein Dokument, welches eine informelle Spezifikation enthält (dies kann ein Verweis auf eine informell spezifizierte Funktionalitätsklasse sein) sowie eine Darstellung der Beziehung zwischen den Sicherheitszielen und den informell formulierten Aussagen;

c) globale Substitutionen;

d) Aussagen in der Reihenfolge der jeweiligen generischen Oberbegriffe;

e) Details über die Sicherheits-Mechanismen;

f) die angestrebte Mindeststärke der Mechanismen;

g) die angestrebte Evaluationsstufe.

B.39 Unter der Überschrift Globale Substitutionen sind alle allgemeinen Substitutionen, die in den Aktions- oder Zielsätzen verwendet wurden, zu definieren und zu erklären.

B.40 Diese Substitutionen werden außer Kraft gesetzt, wo abweichende (im Normalfall spezifischere) Substitutionen als Teil bestimmter Aussagen verwendet werden.

B.41 Wenn ein EVG auf Eigenschaften seiner realen oder angenommenen Einsatzumgebung angewiesen ist, um korrekt zu arbeiten, so muß dies in der Produkt-Beschreibung oder im Abschnitt über die Sicherheitspolitik des Claims-Dokumentes niedergelegt sein. Im Evaluationsprozess wird dann angenommen, daß diese Einschränkungen zutreffen.

B.42 Jede dieser Einschränkungen/Annahmen muß entweder in natürlicher Sprache oder in der Claims-Sprache formuliert sein (unter Verwendung des Umgebungs-Indikators des Aktionssatzes). Wo Mehrdeutigkeiten existieren (da die natürliche Sprache verwendet

wurde), wird der Evaluator die Einschränkungen/Annahmen dergestalt interpretieren, daß sie in Übereinstimmung mit anderen Annahmen und Aussagen sind.

B.43 Einige Aussagen können ihre Gültigkeit selbst dann behalten, wenn eine bestimmte Behauptung nicht zutrifft. Wo dies der Fall ist, muß in natürlicher Sprache angegeben werden, welche Aussagen selbst dann wahr sind, wenn die Behauptung nicht zutrifft.

B.44 Ein Beispiel für eine Behauptung (in natürlicher Sprache):

Die RAM-Backup-Batterie darf nicht aus der Sicherheitsplatine entfernt oder unter ihre Mindestbetriebsspannung entladen werden.

Format einzelner Aussagen

B.45 Wenn eine Substitution in Aktions- oder Zielsätzen, die für die Formulierung einer Aussage verwendet wird, im globalen Substitutionsabschnitt des Claims-Dokumentes weder identifiziert noch definiert wurde, so muß sie in natürlicher Sprache definiert werden, und zwar direkt nach der Aussage, in der sie verwendet wird.

Tabelle B.1 Aussage-Zielsätze und generische Oberbegriffe

		Identifizierung und Authentisierung	Zugriffskontrolle	Beweissicherung	Protokollauswertung	Wiederaufbereitung	Unverfälschtheit	Zuverlässigkeit der Dienstleistung	Übertragungssicherg.
1	Protokollinformationen	X	X	X	X	X	X	X	X
2	Identität eines angeforderten Prozesses	X	X	X	X			X	X
3	Identität von {B,P}, der einen Prozeß anfordert	X	X	X	X			X	X
4	Identität von {B,P} der ein Objekt anfordert	X	X	X	X			X	X
5	Identität eines ausgeführten Prozesses	X	X	X	X			X	X
6	Rückweisung eines angeforderten Prozesses	X	X	X	X			X	X
7	Identität eines angeforderten Objekts	X	X	X	X			X	X
8	Identität eines gewährten Objekts	X	X	X	X		X	X	X
9	Identität eines verweigerten Objekts	X	X	X	X			X	X
10	Zugriffseinstellung eines Benutzers		X						X
11	Zugriffseinstellung eines Prozesses		X						X
12	Zugriffseinstellung von {B,P}		X						X
13	Zugriffseinstellung eines Objekts		X						X
14	Objektzugriff, der {B,P} gewährt wurde	X	X	X	X				X
15	Objektzugriff durch {B,P}	X	X	X	X				X
16	Objektaktionen, die von {B,P} ausgeführt wurden		X	X	X				X
17	Faktoren, die die Benutzer-Zugriffseinstellung betr.		X						X
18	Faktoren, die die Prozeß-Zugriffseinstellung betreffen		X						X
19	Faktoren, die die {B,P}-Zugriffseinstellung betreffen		X						X
20	Faktoren, die die Objekt-Zugriffseinstellung betreffen		X						X
21	Löschen von Informationen aus Objekt					X			X
22	Sicherheitsattribute eines Objekts	X	X	X	X	X	X	X	X
23	Korrektheit der Sicherheitsattribute eines Objekts						X		X
24	Sicherheitsattribute eines kombinierten Objekts		X				X		X
25	Sicherheitsattribute eins aufgeteilten Objekts		X				X		X
26	Zugriffsgewährung führt nicht zu Verklemmung							X	X
27	Verklemmung kann erkannt werden							X	X
28	Zugriffsgewährung führt nicht zu Livelock							X	X
29	Livelock kann erkannt werden							X	X
30	Objekte besitzen identische Sicherheitsattribute		X				X		X
31	Zeitkritische Aussage							X	
32	Beschleunigte oder verzögerte Aussage							X	
33	Zeitabhängige Aussage							X	
34	Aussage bzgl. Umgehung	X	X	X	X	X	X	X	X
35	Aussage bzgl. Deaktivierung	X	X	X	X	X	X	X	X
36	Aussage bzgl. Korrumpierung	X	X	X	X	X	X	X	X

Tabelle B.2 Aussage-Zielsätze und zulässige Substitutionen

		Zugriffseinstellung	Zugriffstyp	Protokollinformation	Aussage	Objekt	Prozeß	Sicherheitsattribut	Sicherheitsrelev. Ereignis	Benutzer	{Benutzer,Prozeß}
1	Protokollinformationen			X			X				
2	Identität eines angeforderten Prozesses					X					
3	Identität von {B,P} der einen Prozeß anfordert					X					X
4	Identität von {B,P} der ein Objekt anfordert		X			X					X
5	Identität eines ausgeführten Prozesses					X					
6	Rückweisung eines angeforderten Prozesses					X					
7	Identität eines angeforderten Objekts		X			X					
8	Identität eines gewährten Objekts		X			X					
9	Identität eines verweigerten Objekts		X			X					
10	Zugriffseinstellung eines Benutzers	X								X	
11	Zugriffseinstellung eines Prozesses	X				X					
12	Zugriffseinstellung von {B,P}	X									X
13	Zugriffseinstellung eines Objekts	X				X					
14	Objektzugriff, der {B,P} gewährte wurde		X			X					X
15	Objektzugriff durch {B,P}		X			X					X
16	Objektaktionen, die von {B,P} ausgeführt wurden					X					X
17	Faktoren, die die B-Zugriffseinstellung betreffen	X								X	
18	Faktoren, die die P-Zugriffseinstellung betreffen	X				X					
19	Faktoren, die die {B,P}-Zugriffseinst. betreffen	X									X
20	Faktoren, die die Objekt-Zugriffseinst. betreffen	X				X					
21	Löschen von Informationen aus Objekt					X					
22	Sicherheitattribute eines Objekts					X		X			
23	Korrektheit der Sicherheitsattribute eines Objekts					X		X			
24	Sicherheitsattribute eines kombinierten Objekts					X		X			
25	Sicherheitsattribute eines aufgeteilten Objekts					X		X			
26	Zugriffsgewährung führt nicht zu Verklemmung		X			X					X
27	Verklemmung kann erkannt werden		X			X					X
28	Zugriffsgewährung führt nicht zu Livelock		X			X					X
29	Livelock kann erkannt werden		X			X					X
30	Objekte besitzen identische Sicherheitsattribute					X		X			
31	Zeitkritische Aussage				X						
32	Beschleunigte oder verzögerte Aussage				X						
33	Zeitabhängige Aussage				X						
34	Aussage bzgl. Umgehung				X						
35	Aussage bzgl. Deaktivierung				X						
36	Aussage bzgl. Korrumpierung				X						