Kommentare und Hinweise zum ULD-Anforderungskatalog

(ANLEHNUNG AN DIE CC)

Version	Final_01
Datum	07.03.2003
Kontakt:	mail@datenschutzzentrum.de

I. Einleitung

Das ULD-Gütesiegel bescheinigt, dass die Vereinbarkeit eines Produktes mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde. Auf dieser Grundlage empfiehlt das ULD den Einsatz des Produktes bei den öffentlichen Stellen in Schleswig-Holstein auf Basis des Landesdatenschutzgesetzes (LDSG-SH).

Hersteller- oder Vertriebsfirmen können einen Sachverständigen oder eine sachverständige Prüfstelle, die beim ULD akkreditiert sein müssen, beauftragen. Die Sachverständigen führen die Prüfung des Produktes durch und erstellen dazu ein Gutachten, das vom Hersteller/Vertreiber zusammen mit dem Antrag auf Zertifizierung an das ULD gesendet wird. Ergibt die Nachprüfung durch das ULD keine Hinderungsgründe, so wird das Gütesiegel erteilt.

Mittlerweile hat das ULD erste Erfahrungen bei dem Umgang mit Gutachten gesammelt. Hervorzuheben ist die Bedeutung der Produktdokumentation. Auf Grundlage der Erkenntnis, dass moderne IT-Produkte oft eine Vielzahl von Konfigurations- bzw. Einstellungsmöglichkeiten offenlassen, legen wir erheblichen Wert auf eine umfassende Aufklärung der Administratoren und Benutzer, wie das Produkt datenschutzgerecht zu nutzen ist. Wir konnten feststellen, dass eine solche Dokumentation – analog zu den „Beipackzetteln“ in der pharmazeutischen Industrie – mit Hinweisen auf die “richtige“ Anwendung sowie zu „Risiken und Nebenwirkungen“ häufig nicht vorhanden ist. Diese Defizite müssen vom Gutachter erkannt und vom Produkthersteller vor der Zertifizierung beseitigt werden.

Das Gutachten muss sich an den Prüfhinweisen zum Gütesiegel orientieren, die derzeit aus den Anforderungen an die Produktdokumentation sowie dem Anforderungskatalog zum Datenschutzgütesiegel für IT-Produkte bestehen. Beide werden regelmäßig fortgeschrieben. Die in diesem Text enthaltenen Hinweise und Kommentare dienen dazu, die bestehenden Evaluationskriterien zu den Common Criteria (CC), einem international harmonisierten und standardisierten Katalog von IT-Sicherheitskriterien, in Beziehung zu setzen.

Abschnitt III gibt eine kurze Einführung zum Verfahren der Evaluation nach den CC und vergleicht es mit dem Evaluationsverfahren für das Datenschutzgütesiegel. In Abschnitt IV wird dargestellt, wie sich die technischen Evaluationskriterien nach dem Anforderungskatalog in die CC-Terminologie übersetzen lassen: Wo CC-Familien und –Klassen mit den Anforderungen nach Datenschutzgütesiegel zusammenhängen, werden diese benannt. Sofern keine direkte Ableitung möglich ist, werden – wo sinnvoll – neue Familien und/oder Klassen eingeführt.

Aufgrund der hohen Komplexität der Common Criteria, die sich durch Abhängigkeiten zwischen den einzelnen Prüfkriterien ausdrücken, können in diesem ersten Schritt noch nicht alle Zusammenhänge zwischen verschiedenen Familien und Klassen nach CC dargestellt werden. Die hier gegebenen Hinweise haben vielmehr die Aufgabe, eine erste Übersetzung des Anforderungskatalogs in Common Criteria vorzunehmen. Sachverständige, die sich bereits in den CC auskennen, werden hier Vorteile haben. Eine Rückkopplung der Erfahrungen, die künftig mit dem ULD-Anforderungskatalog in einer CC-Übersetzung gewonnen werden, in die weitergehende Standardisierung dieser internationalen Kriterien ist vorgesehen.

Die Erstellung von Gutachten in der Nomenklatur der CC ist nicht trivial; insbesondere ist die Darstellung des Datenschutzes bisher nur in geringen Teilen standardisiert. Wir empfehlen Gutachtern dringend, vor der Anwendung von CC mit dem ULD zur Abstimmung in Kontakt zu treten.

Im Gegensatz zu üblichen technischen („TÜV“-)Prüfungen, bei denen ein Vergleich von Soll- und Ist-Werten durchgeführt wird, muss man im Bereich des Datenschutzes durch Interpretation von Gesetzesvorgaben zunächst einen Prüfrahmen ermitteln. Die Erteilung des Prüfsiegels kann nur dann erfolgen, wenn das Produkt einschließlich seiner Dokumentation in seiner Einsatzumgebung einen datenschutzgerechten Einsatz zulässt. Erfahrungsgemäß kritisch ist die Abwägung, welcher Stand der Technik für eine datenschutzgerechte Umsetzung von Anforderungen an das Produkt möglich und zumutbar ist. Hier ist die Erfahrung des Gutachters gefragt, in dessen Verantwortung die Forderung an den Produkthersteller liegt, eine möglichst optimale Umsetzung anzubieten.

Bei bisherigen Begutachtungen des ULD im Bereich des Datenschutzes konnten wir feststellen, dass der rechtliche Prüfrahmen stark von der Einsatzumgebung des Produktes abhängig ist. Eine Datenbank kann in einem Kontext beispielsweise zulässig und rechtskonform sein, in einem anderen jedoch nicht. Aus diesem Grund wird stets die Dokumentation des Produktes einschließlich aller Konfigurationsparameter als Grundlage der Begutachtung gefordert. Auch der Ansatz, an die Produktdokumentation gewisse Mindeststandards hinsichtlich Umfang und Qualität sowie deren Berücksichtigung bei der Begutachtung zu stellen, lässt sich besser nachvollziehen, wenn das Ziel des Zertifizierungsvorganges transparent ist: Durch die Anleitungen soll durchschnittlich qualifizierten Verfahrensbetreuern bzw. Administratoren ein datenschutzgerechter Einsatz bei vertretbarem Aufwand möglich sein. Hierzu gehört auch die datenschutzgerechte Revision des Produktes.

Im Bereich des Datenschutz-Gütesiegels muss beachtet werden, dass im Gegensatz zu Sicherheitssiegeln gewisse (rechtlich vorgegebene) Rahmenbedingungen nicht verletzt werden dürfen („K.O.-Bedingungen“); wirtschaftliche Erwägungen und Restrisikobehandlungen sind nur insoweit zulässig, als keine K.O.-Bedingungen verletzt werden.

Das ULD bevorzugt bei der Vergabe des Datenschutzgütesiegels eine technische Umsetzung von Datenschutzanforderungen gegenüber einer organisatorischen Datenschutzmaßnahme. Ein datenschutzgerechter Einsatz ist immer das Ergebnis der sachgerechten Kombination von technischen Maßnahmen, organisatorischer Unterstützung und Dokumentation. Daher gehen die Anforderungen des Datenschutz-Gütesiegels über die rein technische Implementierung hinaus.

Geht man von Mindestanforderungen aufgrund gesetzlicher Regelungen aus, so ergibt sich, dass die Prüftiefe durch den Hersteller nicht beliebig ausgewählt werden kann, sondern ein gewisses Mindestmaß erreichen muss. Abhängig von Einsatzkontext und Produktart ist eine unterschiedliche Tiefe der begutachtenden Prüfung angezeigt: Während beispielsweise ein mechanischer Aktenvernichter vergleichsweise schnell geprüft werden kann, weil nur wenige datenschutzrechtliche Fragen berührt werden und nur wenige Missbrauchsmöglichkeiten gegeben sind, so erfordert ein komplexes Datenbanksystem für die Verwaltung personenbezogener Daten eine intensive Prüfung, die insbesondere die Zugriffsrechte und die Kommunikation mit dem darunterliegenden Betriebssystem betrachten muss.

Das Beispiel macht deutlich, dass die Prüfkriterien für die Begutachtung eines Produktes stets den vom Produkt berührten Rechtsrahmen abdecken müssen und die Prüftiefe dem jeweiligen Produkt und seinem Einsatzkontext angepasst werden müssen. Es lassen sich bisher sechs Parameter bestimmen, die die Prüftiefe beeinflussen:

- Komplexität des Verfahrens bzw. Produktes und seiner Anwendung
- Komplexität der Technik des Produktes
- Komplexität der Rechtsgebiete, die die Datenverarbeitung regeln
- Sensibilität der verarbeiteten Daten
- Geforderte Einsatzumgebung aus technischer Sicht
- Geforderte Einsatzumgebung aus organisatorischer Sicht

Während die ersten vier Parameter die Prüftiefe nicht verringern, aber in ungünstigen Fällen erhöhen können, kann eine in der Produktdokumentation geforderte bzw. definierte sichere Einsatzumgebung mit guten technischen und organisatorischen Maßnahmen dazu führen, dass bei der Prüftiefe Abstriche gemacht werden können. Der Parameter „Sensibilität der Daten“ beinhaltet die rechtlich begründete Sensibilität der durch die Analyse gefundenen Datenarten, die nicht nur von der Einsatzumgebung, sondern auch vom Produktdesign abhängt. Diese Beurteilung ist ein Ergebnis der interdisziplinären und durch wiederholte Abstimmungen geprägten Zusammenarbeit des juristischen und des technischen Gutachters.

In Abhängigkeit von der vom Gutachter vorläufig festgelegten Prüftiefe kann der Übergang zwischen der Prüfung der Anforderungen und der Bewertung für ein IT-Produkt bereits auf einer höheren Abstraktionsebene erfolgen. Bei hohen Prüftiefen ist zunächst eine tiefergehende Detailbetrachtung erforderlich, bevor eine abschließende

Bewertung erfolgen kann.

Das ULD hat sich entschlossen, die Dokumentation der technischen Überprüfung an die Nomenklatur der Common Criteria anzulehnen, da hier den Gutachtern ein systematisches Abarbeiten von Prüffeldern in einer baumartigen Struktur ermöglicht wird.

II. Möglichkeiten von Common Criteria

Vor einer Umsetzung der o.g. Kriterien in dieses Rahmenwerk werden im Folgenden die CC kurz umrissen.

Die Common Criteria sind nicht nur eine Sammlung von IT-Sicherheitskriterien, sondern definieren zugleich ein Prüfungsschema, das ganz ähnlich wie die Prüfung des Gütesiegels aufgebaut ist:

Zunächst werden Umfang, Einsatzgebiete und Zweck des Produktes beschrieben, um das Produkt von seiner Umwelt genau abgrenzen zu können. In der Notation der CC heißt eine Prüfung *Evaluation* und das Produkt *Evaluationsgegenstand* (EVG, engl. *target of evaluation*, TOE).

In einem zweiten Schritt werden Bedrohungen, die Annahmen über die Sicherheit der Umgebung und zu beachtende organisatorische Regelungen untersucht. Beispiele für diese Begriffe sind der Verlust von Daten durch Stromausfall (Bedrohung), ein gesicherter Raum für IT-Server (Annahme) und Protokolierungsanforderungen der Datenschutzgesetze (organisatorische Regelungen). Um diese Punkte untersuchen zu können, müssen die Arten der verarbeiteten Daten bestimmt werden.

Anhand der Bedrohungen, Annahmen und geforderten organisatorischen Regelungen werden im dritten Schritt so genannte *Sicherheitsziele* bestimmt, die das Produkt oder seine Einsatzumgebung sicherstellen muss. Diese Sicherheitsziele sind auf einem abstrakten Niveau ohne konkreten Blick auf die Implementierung formuliert. Ein Beispiel für ein Sicherheitsziel ist: „Das Produkt muss sicherstellen, dass Daten nur von dazu autorisierten Benutzern verarbeitet werden." Welche Sicherheitsziele zu verfolgen sind, ergibt sich aus dem Anforderungsprofil und damit indirekt aus der Art der verarbeiteten Daten und den Rechtsgrundlagen dafür.

Durch welche Maßnahmen das Produkt und seine Einsatzumgebung die Vorgaben der Sicherheitsziele erfüllt, wird im vierten Schritt geklärt: Hier werden zu Sicherheitszielen so genannte *Sicherheitsanforderungen* (eng. target security function, TSF) formuliert, die das Produkt oder seine Einsatzumgebung erfüllen müssen. Sicherheitsanforderungen an das Produkt sind rein technischer Natur, während Anforderungen an die Einsatzumgebung auch nicht-technische Anforderungen enthalten können (z.B. die Anforderung, dass Administratoren kompetent und vertrauenswürdig sind). Wichtig ist, an dieser Stelle die Verantwortlichkeiten von Produkt und Einsatzumgebung klar zu trennen und zu benennen. Darüber hinaus formulieren die CC auch Vertraulichkeitsanforderungen, mit denen Umfang und Genauigkeit der Prüfung modelliert werden: Genügen Funktionstests oder ist eine Analyse des Programmquelltextes erforderlich? Innerhalb des Gütesiegelverfahrens bleibt diese Aufgabe dem Gutachter überlassen.

Die technischen funktionalen Sicherheitsanforderungen an ein Produkt sind im nächsten Schritt in der Nomenklatur der CC zu formulieren und ergeben sich aus den Sicherheitszielen. Die CC stellen dazu eine Vielzahl von funktionalen Komponenten bereit, die in unterschiedlichem Detaillierungsgrad die Sicherheitsfunktionen beschreiben. Ein Beispiel dafür ist die Anforderung, eine Benutzerauthentisierung vor jeglicher sicherheitssensibler Operation sicherzustellen.

Im Gütesiegelverfahren entspricht dieser Schritt einer Formulierung von technischen Soll-Anforderungen, die sich aus dem produktspezifischen Anforderungsprofil ergeben. In Abschnitt IV werden technische Anforderungen, die sich aus dem Gütesiegel-Anforderungskatalog ergeben, und funktionale Sicherheitsanforderungen in der

Nomenklatur der CC gegenübergestellt.

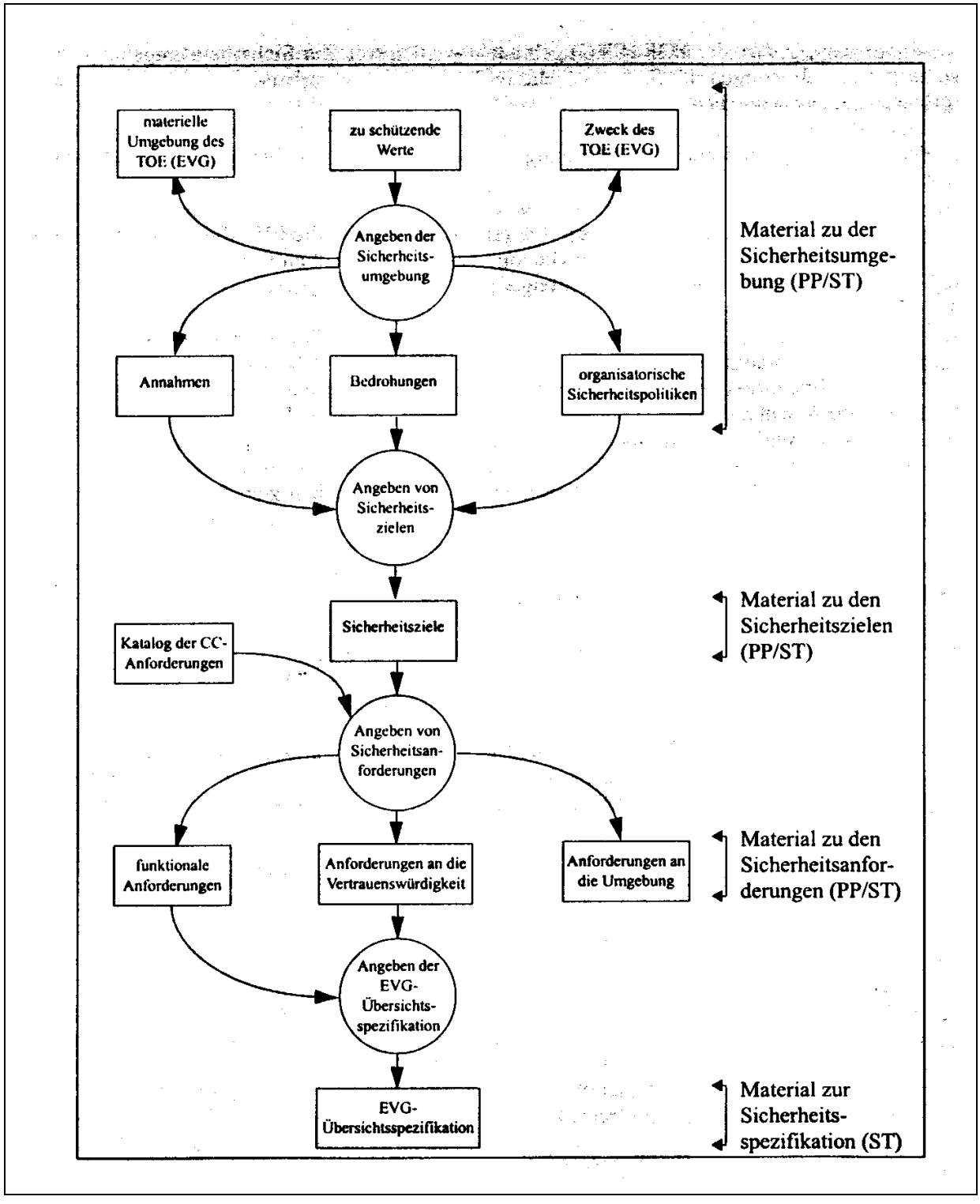
Innerhalb der CC sind aber nicht nur Sicherheitsfunktionen beschrieben, sondern es werden auch Hinweise auf deren Bewertung und notwendige Aktionen des Prüfers gegeben. Besonders wichtig ist, dass Abhängigkeiten zwischen den Sicherheitsanforderungen aufgezeigt werden: Wenn die Forderung nach der Durchsetzung von Zugriffsregeln im Raum steht, muss gleichzeitig auch die sichere Administration der Zugriffsrechte gefordert werden, was wiederum eine zuverlässige Unterscheidung zwischen normalen Benutzern und Administratoren erfordert.

Auch eine Protokollierung der Aktivitäten von Sicherheitsfunktionen kann modelliert werden. Daher weist jede Sicherheitsanforderung auf spezifische Protokoll- und Managementaktivitäten hin, die ggf. ebenfalls zu prüfen sind.

Die bisherige Beschreibung bezieht sich auf die Prüfung eines konkreten Produktes. Soll eine Vielzahl von gleichartigen Produkten überprüft werden, so wiederholen sich bei den Prüfungen viele Überlegungen, etwa zum Einsatzkontext, den Bedrohungen etc.

Daher erlauben die CC die Erstellung von Schutzprofilen (engl. *protection profiles*), die für eine Produktklasse und typische Einsatzkontexte die Anforderungen zusammenstellen. Solche Schutzprofile können je nach betrachteter Produktklasse und Einsatzkontext unterschiedlich abstrakt sein. Sie erlauben dennoch, grundlegende und von der konkreten Implementierung unabhängige Überlegungen „vor die Klammer zu ziehen“. Die Korrektheit und inhaltliche Stringenz von Schutzprofilen lässt sich ihrerseits in einem Zertifizierungsprozess überprüfen.

Als Beispiel hierfür seien die Schutzprofile zu *Benutzerbestimmbarer Informationsflusskontrolle (BISS)*, die Anforderungen an ein System beschreiben, das den Informationsfluß für den Benutzer transparent kontrolliert, genannt. Hier werden auch Überlegungen zur Informationsflusspolitik gemacht. Hintergrund sind Datenschutzanforderungen, die die Vertraulichkeit von Daten auch gegen den Willen des rechtmäßigen Benutzers des IT-Systems garantieren müssen.



Der Evaluationsprozess in den CC (Quelle: BSI, Common Criteria, Version 2.1)

Im folgenden Kapitel wird ein grober Umsetzungsrahmen der bisherigen ULD-Kriterien in die Nomenklatur der CC vorgeschlagen. Dieser ist aufgrund der hohen Komplexität der CC mit den zum Teil umfangreichen Abhängigkeiten zwischen einzelnen Kriterien nicht vollständig und mit den spezifischen Anforderungen an einzelne Produktklassen durch Protection Profiles zu ergänzen.

Wir erwarten, möglichst im Rahmen der im eRegion Programm geförderten Gütesiegelverfahren erste Definitionen von typischen Anwendungs-PPs zu erhalten.

Entsprechend qualifizierten Gutachtern legen wir nahe, in Abstimmung mit dem ULD möglichst frühzeitig die Nomenklatur der CC in ihren Gutachten anzuwenden, um die Nachprüfbarkeit zu vereinfachen und die Fortschreibung der Kriterien zu unterstützen.

III. Modellierung der Anforderungen mit Hilfe der Common Criteria

Dieses Dokument stellt einen ersten Ansatz der Umsetzung des ULD-Anforderungskatalogs in CC-Nomenklatur dar. Nicht alle Kriterien aus diesem Katalog sind jedoch technisch relevant und direkt in CC umsetzbar. Bislang ist nur eine vorläufige Überprüfung der Kriterien durchgeführt worden. Die genannten Referenzen ULD – CC sind daher als Beispiele einer Umsetzung anzusehen.

Die in Kapitel II dargestellte Struktur ist hier an technische Zusammenhänge gebunden wiedergegeben – die zu den jeweiligen technischen Prüfpunkten zuzuordnenden Teilaspekte aus Kapitel II sind jeweils benannt.

Bei einer Prüfung ist i.d.R. mindestens auf die „Bestandteile“ einzugehen; einzelne Prüfpunkte sind von dem Untersuchungsgegenstand und später zu erstellenden Profilen (Protection Profiles) abhängig und geben den Detaillierungsgrad der Prüfung wieder.

Die im Rahmen der Gütesiegel-Evaluierung notwendige Prüftiefe lässt sich nicht ohne weiteres mit den Evaluationsleveln der Common Criteria vergleichen: Einerseits erfordert die Gütesiegel-Evaluation einen teilweise sehr detaillierten Blick auf die Dokumentation der Algorithmen, beschränkt sich aber andererseits an anderen Punkten auf die abstrakte Beschreibung des Datenflusses. In der Nomenklatur der Common Criteria entspricht dies einer Prüfung auf dem Niveau EAL 1+ (Prüfung ohne Zugrundelegung z.B. formaler Verifikationsverfahren). Die Umsetzung der Gütesiegel-Prüftiefe geschieht nicht nur durch Auswahl der zu prüfenden Kriterienklassen, sondern auch durch die Auswahl der zu prüfenden Elemente der Kriterienklassen, die mit steigendem Detaillierungsgrad immer konkreter werden.

Die Gütesiegel-Vorgehensweise entspricht somit nicht der üblichen Herangehensweise bei einer Zertifizierung nach den Common Criteria, stellt aber eine problemadäquate Anpassung an die Bedürfnisse einer Datenschutzprüfung im Rahmen des Gütesiegelverfahrens dar.

Datensparsamkeit

Die datenschutzrechtlichen Grundlagen:

Stelle im Anforderungskatalog	Beschreibung
Komplex 1: Grundsätzliche technische Ausgestaltung von IT-Produkten *1.1 Datensparsamkeit*	• Bestehen Möglichkeiten, dass Betroffene anonym oder pseudonym agieren oder sie wenigstens nachträglich zu anonymisieren oder pseudonymisieren?
1.2 Frühzeitiges Löschen, Anonymisieren oder Pseudonymisieren, wenn Daten noch erforderlich, aber Personenbezug verzichtbar	• Wie werden [...] Anonymisierung und Pseudonymisierung umgesetzt (automatisch / in welchen Abhängigkeiten)? • Wird die Pseudonymisierung/Anonymisierung zum frühest möglichen Zeitpunkt vorgenommen? • Wovon hängt der Zeitpunkt der Anonymisierung oder Pseudonymisierung ab? • Sind geeignete Maßnahmen ergriffen worden, um die Zuordnungsfunktion bei einer Pseudonymisierung zu sichern? Ist die Zuordnungsfunktion geeignet, oder besteht die Gefahr, mit nur wenig Zusatzwissen einzelne Daten depseudonymisieren zu können (etwa bei einer Pseudonymisierung durch Vertauschen von Namensbuchstaben etc.)?
Komplex 2: Zulässigkeit der Datenverarbeitung *2 Zulässigkeit der Datenverarbeitung* *2.1 Allgemeine Voraussetzung der Zulässigkeit (z.B. §§ 11-16 LDSG, §§ 67a ff. SGB X, §§ 4, 28 ff. BDSG)* *2.1.1 Vorliegen der gesetzlichen Voraussetzungen*	• Inwieweit sind Pseudonymisierung- bzw. Anonymisierungsgebote (z.B. §22 LDSG) zu beachten?
2.2.2 Speicherung bzw. weitere Verarbeitung (§ 13 Abs. 2-6 LDSG, § 67b SGB X, §§ 28-30 BDSG) *2.2.2.1 Sämtliche Anforderungen, die sich aus §§ 5 Abs. 1 sowie § 6 Abs. 1 LDSG ergeben.* *2.2.2.3 Erleichterung der Umsetzung des Trennungsgebotes nach § 11 Abs. 4 LDSG und § 15 IFG*	• Gibt es Verfahren zur automatisierten Pseudo-/Anonymisierung (siehe auch Abschnitt 1.2)?
2.2.3 Übermittlung (§§ 14-16 LDSG, §§ 67d-78 SGB X, §§ 28, 29 BDSG)	• Sind bei der Übermittlung an Dritte Maßnahmen vorgesehen, um Daten zu anonymisieren oder pseudonymisieren (§11 Abs. 6 LDSG) (siehe auch Abschnitt 1.2)?

Stelle im Anforderungskatalog	Beschreibung
3.2.2 Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens (§ 2 Abs. 2 Nr. 7 LDSG, § 67 Abs. 8a SGB X, § 3 Abs. 6a BDSG)	• Ist eine Pseudonymisierung von Daten für Zwecke der Forschung (§ 22 Abs. 1 LDSG) geboten? • Ist eine Pseudonymisierung von Daten im Rahmen der Datenverarbeitung und Übermittlung (§ 11 Abs. 6 LDSG) gefordert oder geboten?

Bestandteile

REQ-APNYM-a	Betroffene können anonym agieren
REQ-APNYM-b	Betroffene können pseudonym agieren
REQ-APNYM-c	Nachträgliche Anonymisierung
REQ-APNYM-d	Nachträgliche Pseudonymisierung

REQ-APNYM-a Betroffene können anonym **agieren**

FPR_ANO.1.1 / FPR_ANO.2.1
Die TSF müssen sicherstellen, dass [Zuweisung: Benutzer- und/oder Subjektmenge] nicht in der Lage sind, die mit [Zuweisung: Liste von Subjekten und/ oder Operationen und/oder Objekten] verbundenen tatsächlichen Benutzernamen festzustellen.

FPR_ANO.2.2 (inkl. FPR_ANO.2.1)
Die TSF müssen eine Liste bestimmter Dienste für bestimmte Subjekte bereitstellen, ohne einen Verweis auf den tatsächlichen Benutzernamen zu verlangen.

REQ-APNYM-b Betroffene können pseudonym agieren

FPR_PSE.1.1 / FPR_PSE.2.1 / FPR_PSE.3.1
Die TSF müssen sicherstellen, dass die wahre Identität eines Benutzers, der mit einem Asset bzw. Prozess verbunden ist, von anderen Benutzern ***nicht*** erkannt wird.

FPR_PSE.1.2 / FPR_PSE.2.2 / FPR_PSE.3.2 (inkl. FPR_PSE.1.1 / FPR_PSE.2.1 / FPR_PSE.3.1)
Die TSF müssen in der Lage sein, [Zuweisung: Aliasanzahl] Aliasse tatsächlicher Benutzernamen den [Zuweisung: Liste der Subjekte] bereitzustellen.

FPR_PSE.1.3 / FPR_PSE.2.3 / FPR_PSE.3.3 (inkl. FPR_PSE.1.2 / FPR_PSE.2.2 / FPR_PSE.3.2)
Die TSF müssen [Auswahl: Alias für den Benutzer festlegen, Alias vom Benutzer annehmen] und verifizieren, dass dieser der [Zuweisung: Aliasmetrik] entspricht.

FPR_PSE.2.4 (inkl. FPR_PSE.2.3)
Die TSF müssen eine Funktion zur Verfügung stellen, die den Berechtigten unter bestimmten Voraussetzungen erlaubt, eine Benutzeridentität, basierend auf dem bereitgestellten Alias, festzustellen.

FPR_PSE.3.4 (inkl. FPR_PSE.3.3)
Die TSF müssen einen Alias für den tatsächlichen Benutzernamen bereitstellen, der unter bestimmten Bedingungen identisch mit einem früher bereitgestellten Alias sein muss, ansonsten darf der bereitgestellte Alias keine Beziehung zu früher bereitgestellten Aliassen haben.

REQ-APNYM-c Nachträgliche Anonymisierung

REQ-APNYM-d Nachträgliche Pseudonymisierung

Erfassung personenbezogener Daten

Die datenschutzrechtlichen Grundlagen:

Stelle im Anforderungskatalog	Beschreibung
Komplex 1: Grundsätzliche technische Ausgestaltung von IT-Produkten *1.1 Datensparsamkeit*	• Ist ein vollständiger Verzicht auf personenbezogene Daten möglich? Wenn nein, warum nicht? • Welche (Kombinationen von) personenbezogenen Daten sind wirklich erforderlich? Wovon hängt dies ab?
Komplex 3: Technisch-organisatorische Maßnahmen: Begleitmaßnahmen zum Schutz der Betroffenen *3.2 Spezifische Pflichten* *3.2.3 Technische Umsetzung von Transparenz- und Beteiligungsgeboten für die Betroffenen bei besonderem Technikeinsatz* *3.2.3.1 bei Chipkarten (§ 18 Abs. 2 LDSG, § 6c BDSG)*	• Sind die Verarbeitungsgeräte so gestaltet, dass Verarbeitungsvorgänge sowie Art und Umfang personenbezogener Daten jederzeit erkennbar sind?

Bestandteile

REQ-PDATA-a	Verzicht auf personenbezogene Daten

REQ-PDATA-a Verzicht auf personenbezogene Daten

NN
Die TSF können teilweise auf personenbezogene Daten verzichten.

NN
Die TSF verzichten vollständig auf personenbezogene Daten.

Zweckbestimmung

Die datenschutzrechtlichen Grundlagen:

Stelle im Anforderungskatalog	Beschreibung
Komplex 2: Zulässigkeit der Datenverarbeitung *2.1 Allgemeine Voraussetzung der Zulässigkeit (z.B. §§ 11-16 LDSG, §§ 67a ff. SGB X, §§ 4, 28 ff. BDSG)* *2.1.3 Einwilligung (§ 12 LDSG, § 67b Abs. 2, 3 SGB X, vgl. § 4a BDSG)*	• Enthält eine Einwilligungsformulierung hinreichend bestimmte Angaben zu verarbeitenden Stellen/Empfängern, Art der Verarbeitung, verarbeitete Daten und Zweck-bestimmung?
Komplex 2: Zulässigkeit der Datenverarbeitung *2.2 Zulässigkeit in den einzelnen Phasen der Datenverarbeitung* *2.2.2 Speicherung bzw. weitere Verarbeitung (§ 13 Abs. 2-6 LDSG, § 67b SGB X, §§ 28-30 BDSG)* *2.2.2.2 Sicherstellung der Zweckbindung*	• Wie wird der Zweck dokumentiert, für den die personenbezogenen Daten erhoben wurden? Siehe auch Abschnitt 2.2.3 und 2.2.4.
2.2.4 Zweckbindung (§ 13 Abs. 2 LDSG, § 67c Abs. 1 SGB X) und Zweckänderung (§ 13 Abs. 3 LDSG, § 67c Abs. 2 SGB X, § 28 Abs. 2, 3 BDSG)	• Gibt es eine revisionssichere Protokollierung der Verarbeitung, um Zweckänderungen nachweisen zu können? • Wird die Zweckbindung dadurch garantiert, dass unnötige personenbezogene Daten vermieden werden oder ihre Verkettbarkeit und damit eine zweckändernde Nutzung erschwert oder verhindert wird? • Gibt es eine Kennzeichnung von Datensätzen mit entsprechenden Zwecken sowie Zugriffsrechte, die andere Auswertungsmethoden oder eine Übermittlung einschränken?

Bestandteile

REQ-ZWECK-a	Kennzeichnung der Datensätze mit dem Attribut „Zweck“ und die entspr. Zugriffskontrolle.
REQ-ZWECK-b	Zweckbindung ist automatisiert und überwacht.
REQ-ZWECK-c	Unverkettbarkeit

REQ-ZWECK-a: Kennzeichnung der Datensätze mit dem Attribut „Zweck“ und die entspr. Zugriffskontrolle

NN
Die TSF müssen einen Mechanismus zur Kennzeichnung der personenbezogenen Daten mit dem Attribut „Zweck“ zur Verfügung stellen.

Management: (Klasse FMT)
Folgende Aktionen kommen für Managementfunktionen in Betracht:

- Benutzer mit Zugriffsrechten auf personenbezogene Daten können das Attribut „Zweck“ ändern,
- nur besonders dazu autorisierte Benutzer können das Attribut „Zweck“ ändern.

Protokollierung (Klasse FAU):
Zweckänderungen können protokolliert werden.

REQ-ZWECK-b: Zweckbindung ist automatisiert

NN
Die TSF müssen einen Mechanismus zur Verfügung stellen, mit dem Benutzer bei zweckwidrigen Datennutzungen gewarnt werden.

NN
Die TSF müssen einen Mechanismus zur Verfügung stellen, mit dem eine zweckwidrige Datennutzung unterbunden´wird.

Protokollierung (Klasse FAU):
Der Versuch einer zweckwidrigen Datennutzung kann protokolliert werden.

REQ-ZWECK-c: Wird die Zweckbindung dadurch garantiert, dass unnötige personenbezogene Daten vermieden werden oder ihre Verkettbarkeit und damit eine zweckändernde Nutzung erschwert oder verhindert wird?

NN
Die TSF müssen Mechanismen bereitstellen, um den Umfang der verarbeiteten Daten parametrisieren zu können (z.B. Umfang von Datenprofilen) .

NN
Die TSF bieten Möglichkeiten zur Verhinderung einer Verkettbarkeit der personenbezogenen Daten.

Trennungsgebot

Die datenschutzrechtlichen Grundlagen:

Stelle im Anforderungskatalog	Beschreibung
Komplex 2: Zulässigkeit der Datenverarbeitung *2.2 Zulässigkeit in den einzelnen Phasen der Datenverarbeitung* *2.2.2 Speicherung bzw. weitere Verarbeitung (§ 13 Abs. 2-6 LDSG, § 67b SGB X, §§ 28-30 BDSG)* *2.2.2.3 Erleichterung der Umsetzung des Trennungsgebotes nach § 11 Abs. 4 LDSG und § 15 IFG*	• Wie ist das Trennungsgebot technisch umgesetzt? • Werden schutzwürdige Belange, die einer Weitergabe von untrennbar verbunden Daten entgegenstehen, geprüft?
Komplex 4: *4.2 Auskunft (§ 27 LDSG, §§ 25, 83 SGB X, § 34 BDSG, Art. 12 EU-DSRL)*	• Werden untrennbare Verknüpfung mit personenbezogenen Daten anderer Betroffener vermieden ?

Bestandteile

REQ-TRNGG-a	direkte Technische Umsetzung des Trennungsgebots

REQ-TRNGG-a: direkte Technische Umsetzung des Trennungsgebots

NN
Die TSF stellen Funktionalitäten bereit, Datensätze aufzuteilen und die Teile getrennt zu speichern und zu verarbeiten.

Übermittlung (insbesondere von personenbezogenen Daten)

Die datenschutzrechtlichen Grundlagen:

Stelle im Anforderungskatalog	**Beschreibung**

Komplex 2: Zulässigkeit der Datenverarbeitung
2.2 Zulässigkeit in den einzelnen Phasen der Datenverarbeitung
2.2.3 Übermittlung (§§ 14-16 LDSG, §§ 67d-78 SGB X, §§ 28, 29 BDSG))
	• Erfolgt eine Protokollierung? Sind die datenschutzrechtlichen Vorschriften für die Protokolldaten erfüllt?
	• Erfolgt ein Hinweis bzw. eine Verpflichtung auf die Zweckbindung der erhaltenen Daten (vgl. §§ 15 Abs. 2, 16 Abs. 4 LDSG, § 78 Abs. 2 SGB X, § 4b Abs. 6 BDSG)?
	• Kann eine Zweckbindung technisch überwacht werden und können Daten, die nicht übermittelt werden dürfen, von der Übermittlung ausgeschlossen werden?
	• Wird die Richtigkeit der Empfängeradresse verifiziert? Gibt es Filter für mögliche Adressaten bzw. Adressatenkreise, an die keinesfalls eine Übermittlung erfolgen darf (z.B. durch Sperrung von Empfängeradressen außerhalb des Hauses in einem E-Mail-System)?
	  • Filter für ausgehende Informationen: Gibt es Mechanismen, um eine versehentliche unbefugte Weitergabe oder Offenbarung von Daten/Datenträgern zu verhindern oder zu erschweren, z.B. durch rückstandslose Beseitigung von personenbezogenen (Zusatz-)Daten bei möglicher Herausgabe (z.B. detaillierte Informationen über den Autor in Word-Dokumenten, automatisierte Weitergabe von Zusatzinformationen bei HTTP-Kommunikation durch Voreinstellungen im Webbrowser)?
	  • Gibt es Maßnahmen zur Steigerung der Sensibilität der Verarbeiter, um diese vor unbedachten/unerlaubten Übermittlungen zu schützen?

Komplex 3: Technisch-organisatorische Maßnahmen: Begleitmaßnahmen zum Schutz der Betroffenen *3.1 Abstrakte Pflichten* 3.1.1 § 5 LDSG (bzw. § 78a SGB X od. § 9 BDSG jeweils mit Anhang) *3.1.1.2 Maßnahmen, um zu verhindern, dass Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können (§ 5 Abs. 1 Nr. 2 LDSG)*	• Zu technischen Fragen der Sicherung der Übermittlung siehe auch Abschnitt 2.2.3
3.1.1.4 Weitere technische und organisatorische Maßnahmen (§ 5 Abs. 1 Satz 1 LDSG)	• Wird die Vertraulichkeit von Datenbeständen bei ... Übermittlung ausreichend sichergestellt?

Stelle im Anforderungskatalog	**Beschreibung**
Komplex 4: *4.2 Auskunft (§ 27 LDSG, §§ 25, 83 SGB X, § 34 BDSG, Art. 12 EU-DSRL)*	• Gibt es eine Protokollierung bei der Übermittlung personenbezogener Daten?
4.3 Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegendarstellung (§§ 28, 29 LDSG, § 84 SGB X, § 35 BDSG) *4.3.1 Berichtigung*	• Wie werden Berichtigungen an Empfänger vorangegangener Datenübermittlungen weitergeleitet?
4.3.4 Einwand bzw. Widerspruch gegen die Verarbeitung (§ 29 LDSG, § 84 Abs. 1a SGB X, § 35 Abs. 5 BDSG)	• Wie werden Widersprüche an Empfänger vorangegangener Datenübermittlungen weitergeleitet?

Bestandteile

REQ-TRNSF-a	Umsetzung der Policies für Informationsfluss von und zu vordefinierten Stellen in der Infrastruktur.
REQ-TRNSF-b	Vollständige Informationsflusskontrolle.
REQ-TRNSF-c	Umsetzung der datenschutzrechtlichen Vorschriften für die Protokollierung der Datenübermittlung.
REQ-TRNSF-d:	Weiterleitung von Berichtigungen und Widersprüchen an die Empfänger von Datenübermittlungen

REQ-TRNSF-a: Umsetzung der Policies für Informationsfluss von und zu vordefinierten Stellen in der Infrastruktur

FDP.IFC.1.1
Die TSF müssen die Policies für Informationsfluss durchsetzen.

REQ-TRNSF-b: Vollständige Informationsflusskontrolle

FDP_IFC.2.1
Die TSF müssen die [Zuweisung: SFP für Informationsflusskontrolle] für [Zuweisung: Liste der Subjekte und Informationen] und alle durch die SFP abgedeckten Operationen, die einen Fluss dieser Informationen zu und von Subjekten bewirken, durchsetzen.

FDP_IFC.2.2
Die TSF müssen sicherstellen, dass alle Operationen, die das Übertragen von TSC-Informationen zu und von Subjekten innerhalb des TSC bewirken, durch eine SFP für Informationsflusskontrolle abgedeckt sind.

REQ-TRNSF-c: Umsetzung der datenschutzrechtlichen Vorschriften für die Protokollierung der Datenübermittlung

NN
Die TSF müssen Umsetzung der datenschutzrechtlichen Vorschriften für die Protokollierung der Datenübermittlung. sicherstellen

Die Klassen FAU_GEN und FAU_SEL sind zu beachten.

REQ-TRNSF-d: Weiterleitung von Berichtigungen und Widersprüchen an die Empfänger von Datenübermittlungen

NN
Die TSF müssen die Auswertung von Protokolldatenbeständen zur Bestimmung von Empfänger und Übermittlungsdatensatz früherer Übermittlungen unterstützen, um diesen Empfängern Informationen über Berichtigungen und Widersprüche übermitteln zu können.

Löschung

Die datenschutzrechtlichen Grundlagen:

Stelle im Anforderungskatalog	Beschreibung
Komplex 2: Zulässigkeit der Datenverarbeitung *2.2 Zulässigkeit in den einzelnen Phasen der Datenverarbeitung* *2.2.5 Löschung nach Wegfall der Erfordernis (§28 Abs. 2 Satz 2 LDSG)*	• Sind Fristen (Löschungsfristen, Wiedervorlagefristen) zu beachten? Wie wird deren Beachtung sichergestellt? • Siehe auch Abschnitt 4.3.2 zu Löschung
Komplex 4: *4.3 Berichtigung, Löschung, Sperrung, Einwand bzw. Widerspruch, Gegendarstellung (§§ 28, 29 LDSG, § 84 SGB X, § 35 BDSG)* *4.3.2 Vollständige Löschung*	• Wird vollständig und irreversibel gelöscht? • Geschieht dies durch physikalisches Löschen auf allen Medien (ohne zusätzliche Kopien, etwa innerhalb einer Funktion zum Rückgängigmachen von Löschungen)? • Ist eine Selektivität des Löschens möglich (z.B. problematisch bei CD-ROM)? • Wird durch Überschreiben gelöscht? Ist die Umsetzung (z.B. Anzahl der Überschreibvorgänge) adäquat? • Wie ist die Umsetzung der Löschung auf Backup-Medien realisiert? • Wie werden Löschungen an Empfänger vorangegangener Datenübermittlungen weitergeleitet? • Wie werden Lösch- und Prüffristen (Wiedervorlage) realisiert oder unterstützt?
Komplex 3: Technisch-organisatorische Maßnahmen: Begleitmaßnahmen zum Schutz der Betroffenen *3.1 Abstrakte Pflichten* *3.1.1 § 5 LDSG (bzw. § 78a SGB X od. § 9 BDSG jeweils mit Anhang)* *3.1.1.2 Maßnahmen, um zu verhindern, dass Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können (§ 5 Abs. 1 Nr. 2 LDSG)*	• Wird die rückstandslose Beseitigung von personenbezogenen Daten von Datenträgern/Geräte(teile)n (z.B. Festplatten, Schreibbänder, Faxbauteile), die an Dritte weitergegeben werden können, gewährleistet oder unterstützt? • Sind Maßnahmen zum Löschen/Sperren/Zerstören der Daten oder Geräte bei unbefugtem Öffnen/Eingriffen (z.B. bei Chipkarten) vorgesehen?
3.2.3 Technische Umsetzung von Transparenz- und Beteiligungsgeboten für die Betroffenen bei besonderem Technikeinsatz *3.2.3.2 bei Videoüberwachung (§ 20 Abs. 2 S. 1 LDSG, § 6b Abs. 2, 4 BDSG)*	• Wird die Einhaltung der gesetzlichen Löschungsfristen für Aufzeichnungen sichergestellt?

Bestandteile

REQ-DELET-a	Wie werden Lösch- und Prüffristen (Wiedervorlage) realisiert oder unterstützt?
REQ-DELET-b	Wird vollständig und irreversibel gelöscht?
REQ-DELET-c	Wird durch Überschreiben gelöscht? Ist die Umsetzung (z.B. Anzahl der Überschreibvorgänge) adäquat?
REQ-DELET-d	Geschieht dies durch physikalisches Löschen auf allen Medien? Ist eine Selektivität des Löschens möglich? (z.B. problematisch bei CD-ROM)?
REQ-DELET-e	Wie ist die Umsetzung der Löschung auf backup-Medien realisiert?
REQ-DELET-f	Entstehen während der Löschung zusätzliche Kopien, etwa innerhalb einer Funktion zum Rückgängig machen von Löschungen?

REQ-DELET-a: Wie werden Lösch- und Prüffristen (Wiedervorlage) realisiert oder unterstützt?

NN
Die TSF müssen **Mechanismen** bereitstellen, um Policies zur fristgerechten Löschung bzw. prüfenden Wiedervorlage vor einer Löschung durchsetzen zu können.

REQ-DELET-b: Wird vollständig und irreversibel gelöscht?

NN
Die TSF müssen eine vollständige und irreversible Löschung ermöglichen.

REQ-DELET-c: Wird durch Überschreiben gelöscht? Ist die Umsetzung (z.B. Anzahl der Überschreibvorgänge) adäquat?

NN
Die TSF müssen die Löschfunktion durch n-maliges Überschreiben durchführen.

NN
Die TSF müssen den Einsatz von speziellen sicheren Algorithmen zum Löschen der Daten erlauben.

REQ-DELET-d: Ist ein physikalisches Löschen auf allen Medien möglich?

NN
Die TSF dürfen eine Aufbewahrung der Daten auf nicht-löschbaren Datenträgern nur unter bestimmten Bedingungen unterstützen.

REQ-DELET-e: Wie ist die Umsetzung der Löschung auf löschbaren Backup-Medien realisiert?
Ist eine Selektivität des Löschens möglich?

NN
Die TSF müssen ein physikalisches Löschen auf allen Medien (u.a. auf Backup-Medien) sicherstellen.

NN
Die TSF müssen die Löschung einzelner Datensätze auf einem Speichermedium erlauben, ohne die anderen gespeicherten Daten zu beeinflussen.

REQ-DELET-f: Entstehen während der Löschung zusätzliche Kopien, etwa innerhalb einer Funktion zum Rückgängig machen von Löschungen?

NN
Die TSF dürfen die Erstellung zusätzlicher Kopien während der Löschung, etwa innerhalb einer Funktion zum Rückgängig machen, nur unter bestimmten Bedingungen zulassen.

Management: (Klasse FMT)
Folgende Aktionen kommen für Managementfunktuionen in Betracht:

- Autorisierte Benutzer können das Datum der Löschung oder der Wiedervorlage ändern,
- Lösch- und Wiedervorlagefristen werden mit Standardwerten initialisiert,
- nur besonders dazu autorisierte Benutzer können diese Standardwerte ändern.
- nur besonders dazu autorisierte Benutzer können Policies zur fristgerechten Löschung bzw. prüfenden Wiedervorlage ändern
- nur besonders dazu autorisierte Benutzer können die technischen Parameter der Löschung (Anzahl der Überschreibungen etc.) ändern

Protokollierung (Klasse FAU):

- Änderungen von Lösch- und Wiedervorlagefristen einzelner Datensätze können protokolliert werden,
- Änderungen der Standardwerte von Lösch- und Wiedervorlagefristen können protokolliert werden
- Löschungen können protokolliert werden

Temporäre Datenbestände

Die datenschutzrechtlichen Grundlagen:

Stelle im Anforderungskatalog	Beschreibung
Komplex 1: Grundsätzliche technische Ausgestaltung von IT-Produkten *1.1 Datensparsamkeit*	• Wird auf Anlegen von temporären Datenbeständen (z.B. unnötige Protokollierung, Parallel- und Zwischenspeicherung) verzichtet bzw. sind diese Datenbestände wirksam gegen unbefugte Zugriffe gesichert?

Bestandteile

REQ-TEMP-a	Es werden keine sensiblen temporären Dateien angelegt.
REQ-TEMP-b	Es werden temporäre Dateien angelegt, die wirksam gegen unbefugten Zugriff gesichert sind.
REQ-TEMP-c	Die temporären Dateien, die während der Verarbeitung angelegt werden, werden gelöscht.

REQ-TEMP-a Es werden keine sensiblen temporären Dateien angelegt

NN
Die TSF müssen verhindern, dass temporäre Dateien angelegt werden.

NN
Die TSF können erlauben, dass temporäre Dateien angelegt werden, die keine personenbezogenen Daten beinhalten.

REQ-TEMP-b: Es werden temporäre Dateien angelegt, die wirksam gegen unbefugte Zugriffe gesichert sind

NN
Die TSF müssen temporäre Dateien gegen unbefugten Zugriff schützen.

REQ-TEMP-c: Die temporären Dateien, die während der Verarbeitung angelegt werden, werden gelöscht

NN
Die TSF müssen sicherstellen, dass jeder Prozess alle von ihm angelegten temporären Dateien nach Abspeicherung der Daten löscht.

NN
Die TSF müssen sicherstellen, dass jeder Prozess alle von ihm angelegten temporären Dateien auch ohne eine Abspeicherung der Daten löscht.

Spezifikation und Schutz der Benutzergeheimnisse

Die datenschutzrechtlichen Grundlagen:

Stelle im Anforderungskatalog	Beschreibung
Komplex 3: Technisch-organisatorische Maßnahmen: Begleitmaßnahmen zum Schutz der Betroffenen *3.1 Abstrakte Pflichten* *3.1.1 § 5 LDSG (bzw. § 78a SGB X od. § 9 BDSG jeweils mit Anhang)* *3.1.1.2 Maßnahmen, um zu verhindern, dass Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können (§ 5 Abs. 1 Nr. 2 LDSG)*	• Ist ein Passwortschutz sicher umgesetzt (z.B. durch Einmalpasswörter (z.B. Challenge-Response), zeitabhängige Passwörter, Schutz gegen Ausspähung oder Erraten, Länge, Vergabe/Wechsel durch Nutzer selbst, automatisierte Beschränkung des Gültigkeitszeitraumes, Einschränkung der Wiederverwendbarkeit, Sperrmöglich-keit bei Fehlversuchen)?

Bestandteile

REQ-PSWD-a	Vorhandene Formen für Benutzergeheimnisse.
REQ-PSWD-b	Sicherheitsrichtlinien für die Gestaltung der Benutzergeheimnisse in der Textform.
REQ-PSWD-c	Erzeugen der Benutzergeheimnisse in der Textform (Passwort).
REQ-PSWD-d	Anwendung der Benutzergeheimnisse.
REQ-PSWD-e	Schutz der Benutzergeheimnisse bei der Eingabe und Verarbeitung gegen unbefugte Zugriffe
REQ-PSWD-f	Schutz der gespeicherten Benutzergeheimnisse gegen unbefugte Zugriffe

REQ-PSWD-a: **Vorhandene Formen für Benutzergeheimnisse**

FIA_UAU_5.1 (teilweise)
Die TSF müssen einen Benutzer anhand von Benutzergeheimnissen in einer oder mehreren Formen authentifizieren können.

REQ-PSWD-b: Sicherheitsrichtlinien für die Gestaltung der Benutzergeheimnisse in der Textform (Passwort)

FIA_SOS.1.1 / FIA_SOS.2.1
Die TSF müssen einen Mechanismus zur Verfügung stellen, der sicher stellen kann, dass die Benutzergeheimnisse bestimmten Qualitätsrichtlinien (*quality metric*) entsprechen.

REQ-PSWD-c: Erzeugen der Benutzergeheimnisse in Textform (Passwort)

FIA_SOS.2.1
Die TSF müssen einen Mechanismus zur Verfügung stellen, der die Benutzergeheimnisse gemäß den gegebenen Qualitätsrichtlinien (quality metric) **erzeugen** kann.

REQ-PSWD-d: **Anwendung der Benutzergeheimnisse**

FIA_SOS.2.2
Die TSF müssen sicherstellen, dass die durch sie generierten **Benutzergeheimnisse** für bestimmte TSF-Funktionen benutzt werden.

REQ-PSWD-e: Schutz der Benutzergeheimnisse bei der Eingabe und Verarbeitung gegen unbefugte Zugriffe

NN
Die TSF müssen sicherstellen, dass die Benutzergeheimnisse bei der Eingabe und Verarbeitung vor eventuellen Angriffen geschützt werden.

REQ-PSWD-f: Schutz der gespeicherten Benutzergeheimnisse gegen unbefugte Zugriffe

NN
Die TSF müssen sicherstellen, dass die gespeicherten Benutzergeheimnisse vor eventuellen Angriffen geschützt werden.

Authentisierung

Die datenschutzrechtlichen Grundlagen:

Stelle im Anforderungskatalog	Beschreibung
Komplex 3: Technisch-organisatorische Maßnahmen: Begleitmaßnahmen zum Schutz der Betroffenen *3.1 Abstrakte Pflichten* *3.1.1 § 5 LDSG (bzw. § 78a SGB X od. § 9 BDSG jeweils mit Anhang)* *3.1.1.2 Maßnahmen, um zu verhindern, dass Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können (§ 5 Abs. 1 Nr. 2 LDSG)*	• Werden Benutzer des Datenverarbeitungssystems vor Benutzung authentisiert?
Komplex 4: Rechte der Betroffenen *4.2 Auskunft (§ 27 LDSG, §§ 25, 83 SGB X, § 34 BDSG, Art. 12 EU-DSRL)*	• In welcher Weise erfolgt eine Authentisierung des Auskunftsberechtigten?

Bestandteile

REQ-AUTHN-a	Benutzer-Authentisierung vor jeder Aktion
REQ-AUTHN-b	Schutz und Verifizieren der Authentisierungsdaten
REQ-AUTHN-c	Authentisierungsdaten für einmaligen Gebrauch
REQ-AUTHN-d	Verschiedenartige Authentisierungsmechanismen
REQ-AUTHN-e	Wiederholung der Authentisierung
REQ-AUTHN-f	Geschützte Rückmeldungen während der Authentisierung
REQ-AUTHN-g	Authentisierung von Auskunftsberechtigten

REQ-AUTHN-a: Benutzer-Authentisierung vor jeder Aktion

FIA_UAU_2.1
Die TSF müssen erfordern, dass jeder Benutzer erfolgreich authentisiert wurde, bevor diesem jegliche andere TSF-vermittelte Aktionen erlaubt werden.

REQ-AUTHN-b: Schutz und Verifizieren der Authentisierungsdaten

NN
Die TSF verhindern einen Einsatz der Klartext-Passwörter zur Authentisierung in einer Netzumgebung.

FIA_UAU_3.1
Die TSF müssen den Gebrauch von Authentisierungsdaten, die von irgendeinem Benutzer der TSF **gefälscht** wurden, erkennen und/oder verhindern können.

FIA_UAU_3.2
Die TSF müssen den Gebrauch von Authentisierungsdaten, die von irgendeinem anderen Benutzer der TSF **kopiert** wurden, erkennen und/oder verhindern können.

REQ-AUTHN-c: Authentisierungsdaten für einmaligen Gebrauch

FIA_UAU_4.1
Die TSF müssen den Wiedergebrauch von Authentifizierungsdaten, die für einen einmaligen Gebrauch bestimmt sind, nach dem ersten Gebrauch verhindern.

REQ-AUTHN-d: Verschiedenartige Authentisierungsmechanismen

FIA_UAU_5.1 (teilweise)
Die TSF müssen Authentisierungsmechanismen für unterschiedliche Formen der Benutzergeheimnisse bereitstellen.

FIA_UAU_5.2
Die TSF müssen die eingegebene Identität eines jeden Benutzers anhand bestimmter Regel authentifizieren.

REQ-AUTHN-e: Wiederholung der Authentifizierung

FIA_UAU_6.1
Die TSF müssen den Benutzer unter bestimmten Bedingungen wieder authentisieren.

REQ-AUTHN-f: Geschützte Rückmeldungen während der Authentifizierung

FIA_UAU_7.1
Die TSF müssen sicherstellen, dass während der Authentisierung nur bestimmte Feedbacks an den Benutzer bereitgestellt werden.

REQ-AUTHN-g: Authentisierung von Auskunftsberechtigten

N.N.
Die TSF müssen Maßnahmen bereitstellen, um Auskunftsberechtigte, die nicht Benutzer des Systems sind, authentisieren zu können.

Zugriffskontrolle

Die datenschutzrechtlichen Grundlagen:

Stelle im Anforderungskatalog	Beschreibung
Komplex 1: Grundsätzliche technische Ausgestaltung von IT-Produkten *1.1 Datensparsamkeit*	• [...] sind diese [temporären] Datenbestände wirksam gegen unbefugte Zugriffe gesichert?
1.3 Transparenz und Produktbeschreibung	• Ist die Transparenz der Datenverarbeitung ([...] Zugriffs-möglichkeiten) gegenüber - Anwendern (Systemadministration und Nutzer) sowie - Betroffenen gewährleistet?
Komplex 2: Zulässigkeit der Datenverarbeitung *2.2 Zulässigkeit in den einzelnen Phasen der Datenverarbeitung* *2.2.4 Zweckbindung (§ 13 Abs. 2 LDSG, § 67c Abs. 1 SGB X) und Zweckänderung (§ 13 Abs. 3 LDSG, § 67c Abs. 2 SGB X, § 28 Abs. 2, 3 BDSG)*	• Gibt es eine Kennzeichnung von Datensätzen mit entsprechenden Zwecken sowie Zugriffsrechte, die andere Auswertungsmethoden oder eine Übermittlung einschränken?
Komplex 3: Technisch-organisatorische Maßnahmen: Begleitmaßnahmen zum Schutz der Betroffenen *3.1 Abstrakte Pflichten* *3.1.1 § 5 LDSG (bzw. § 78a SGB X od. § 9 BDSG jeweils mit Anhang)* *3.1.1.1 Maßnahmen, um Unbefugten den Zugang zu Datenträgern zu verwehren (§ 5 Abs. 1 Nr. 1 LDSG)*	• Können und werden ausreichend detaillierte Zugriffsrechte vergeben? • Sind ggf. Rollenkonzepte (etwa besondere Berechtigungen von Systemadministration und Kontrollrollen wie Leitung, Datenschutzbeauftragtem oder Revision) berücksichtigt?
3.1.1.2 Maßnahmen, um zu verhindern, dass Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können (§ 5 Abs. 1 Nr. 2 LDSG)	• Werden Firewalls oder Intrusion Detection & Response Systems wirkungsvoll gegen unbefugte Zugriffe eingesetzt?
3.1.1.4 Weitere technische & organisatorische Maßnahmen (§ 5 Abs. 1 Satz 1 LDSG)	• Werden ausreichende Maßnahmen zur Sicherstellung der Verfügbarkeit (z.B. Zugriffsrechte [...]) ergriffen?

Bestandteile

REQ-ACCESS-a	Policy für ausgewählte Zugriffskontrolle
REQ-ACCESS-b	Policy für vollständige Zugriffskontrolle
REQ-ACCESS-c	Funktionen der Zugriffskontrolle
REQ-ACCESS-d	Granularität der Zugriffskontrolle

REQ-ACCESS-a: Policy für ausgewählte Zugriffskontrolle

FDP_ACC.1.1
Die TSF müssen die Policies zur Zugriffskontrolle durchsetzen.

REQ-ACCESS-b: Policy für vollständige Zugriffskontrolle

FDP_ACC.2.1
Die TSF müssen die Policy zur Zugriffskontrolle umsetzen und sicherstellen, dass alle durch die Policy abgedeckten Operationen durchgesetzt werden.

FDP_ACC.2.2
Die TSF müssen sicherstellen, dass alle Operationen zwischen jedem Subjekt im TSC und jedem Objekt im TSC durch eine SFP für Zugriffskontrolle abgedeckt sind.

REQ-ACCESS-c: Funktionen der Zugriffskontrolle

FDP_ACF.1.1
Die TSF müssen die Zuweisung: SFP für Zugriffskontrolle für Objekte, die auf Zuweisung: Sicherheitsattribute, genannte Gruppen von Sicherheitsattributen basieren, durchsetzen.

FDP_ACF.1.2
Die TSF müssen die folgenden Regeln durchsetzen, um festzustellen, ob eine Operation zwischen kontrollierten Subjekten und kontrollierten Objekten zulässig ist: Zuweisung: Regeln für den Zugriff zwischen kontrollierten Subjekten und kontrollierten Objekten mittels kontrollierter Operationen mit kontrollierten Objekten.

FDP_ACF.1.3
Die TSF müssen den Zugriff von Subjekten auf Objekte basierend auf den folgenden zusätzlichen Regeln explizit autorisieren: Zuweisung: auf Sicherheitsattributen basierende Regeln, die den Zugriff von Subjekten auf Objekte explizit autorisieren.

FDP_ACF.1.4
Die TSF müssen den Zugriff von Subjekten auf Objekte, basierend auf Sicherheitsattributen mit Regeln, explizit verweigern.

REQ-ACCESS-d: Granularität der Zugriffskontrolle

NN
Die TSF müssen Policies mit feiner Granularität erlauben, die Zugriffsregelung für Objekte bis hin zu einzelnen Datenfelder einer Datenbank ermöglichen.

Management: (Klasse FMT)
Folgende Aktion kommt für Managementfunktionen in Betracht:

- Autorisierte Benutzer können Zugriffskontrollpolicies ändern,

Protokollierung (Klasse FAU):

- Änderungen von Zugriffskontrollpolicies können protokolliert werden
- unberechtigte Zugriffsversuche (Verstöße) können protokolliert werden
- alle Zugriffsversuche können protokolliert werden

Kryptographie

Die datenschutzrechtlichen Grundlagen:

Stelle im Anforderungskatalog	Beschreibung
Komplex 3: Technisch-organisatorische Maßnahmen: Begleitmaßnahmen zum Schutz der Betroffenen *3.1.1.2 Maßnahmen, um zu verhindern, dass Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können (§ 5 Abs. 1 Nr. 2 LDSG)*	▪ Sind verwendete Verschlüsselungsverfahren adäquat umgesetzt?
Komplex 3: Technisch-organisatorische Maßnahmen: Begleitmaßnahmen zum Schutz der Betroffenen *3.2.1 § 6 LDSG, z.B. Verschlüsselung bei tragbaren Computern* *Untersuchungsgegenstand:*	▪ Werden anerkannte und offen gelegte Verschlüsselungsverfahren eingesetzt? ▪ Sind Schlüsselgenerierung und Schlüsselmanagement adäquat realisiert? ▪ Wurden ausreichende Schlüssellängen eingesetzt? ▪ Wurden Maßnahmen vorgesehen, falls sich die verwendeten Verfahren oder Schlüssellängen als unzulänglich herausstellen (z.B. Wechsel des Verfahrens oder seiner Komponenten, umschlüsseln etc.)

Bestandteile bzw. Einzelgebiete der Anforderungen:

REQ-CRYPT-a	Schlüsselmanagement: Generierung kryptographischer Schlüssel
REQ-CRYPT-b	Schlüsselmanagement: Verteilung kryptographischer Schlüssel
REQ-CRYPT-c	Schlüsselmanagement: Zugriff auf kryptographische Schlüssel
REQ-CRYPT-d	Schlüsselmanagement: Zerstörung kryptographischer Schlüssel
REQ-CRYPT-e	Kryptographischer Betrieb

REQ-CRYPT-a: Schlüsselmanagement: Generierung kryptographischer Schlüssel.

FCS_CKM.1.1
Die TSF müssen die kryptographischen Schlüssel gemäß eines spezifizierten Algorithmus zur kryptographischen Schlüsselgenerierung und spezifizierte kryptographische Schlüssellängen, die bestimmten Normen entsprechen, **generieren**.

REQ-CRYPT-b: Schlüsselmanagement: Verteilung kryptographischer Schlüssel

FCS_CKM.2.1
Die TSF müssen die kryptographischen Schlüssel nach einer spezifizierten Methode zur Verteilung des kryptographischen Schlüssels, die bestimmten Normen entspricht, **verteilen**.

REQ-CRYPT-c: Schlüsselmanagement: Zugriff auf kryptographische Schlüssel

FCS_CKM.3.1
Die TSF müssen die zugelassenen Zugriffsarten gemäß einer spezifizierten Zugriffsmethode auf kryptographische Schlüssel, die bestimmten Normen entspricht, durchführen.

REQ-CRYPT-d: Schlüsselmanagement: Zerstörung kryptographischer Schlüssel

FCS_CKM.1.4
Die TSF müssen die kryptographischen Schlüssel nach einer spezifizierten Methode zur Zerstörung des kryptographischen Schlüssels, die bestimmten Normen entspricht, zerstören.

REQ-CRYPT-e: Kryptographischer Betrieb

FCS_COP.1.1
Die TSF müssen die kryptographischen Operationen gemäß eines spezifizierten kryptographischen Algorithmus und kryptographischer Schlüssellängen, die bestimmten Normen entsprechen, durchführen.

Anhang

Stichworte zur Nomenklatur:

Zur Struktur der Common Criteria (CC)

Die CC bestehen aus drei Teilen, die verschiedene Aspekte der Zertifizierung strukturiert wie folgt aufbauen (nach: BSI, Common Criteria, V. 2.1, 1999)

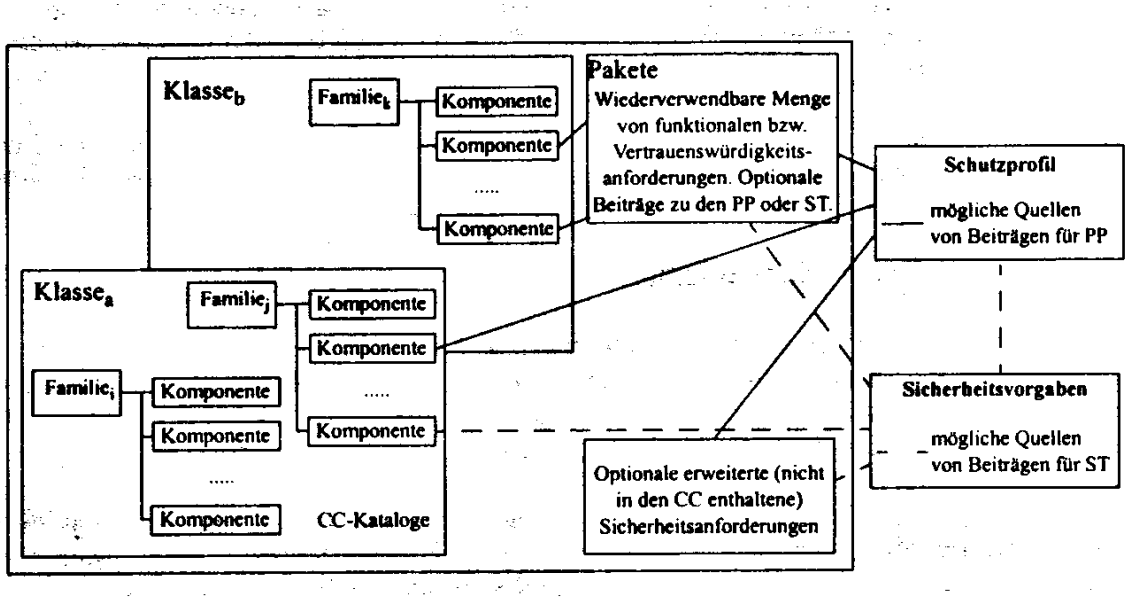
	Anwender	**Entwickler**	**Evaluatoren**
Teil 1 Einführung und allgemeines Modell	Hintergrundinformationen und Nachschlagewerk; allgemeine Anleitung für PP	Hintergrundinformationen und Nachschlagewerk für die Entwicklung von Anforderungen und bei der Formulierung von Sicherheitsspezifikationen für TOE (EVG)	Hintergrundinformationen und Nachschlagewerk; allgemeine Anleitung für PP und ST
Teil 2 Funktionale Sicherheitsanforderungen	Anleitung und Nachschlagewerk für die Darlegung von Aussagen zu Anforderungen an Sicherheitsfunktionen	Nachschlagewerk bei der Interpretation von Darlegungen von funktionalen Anforderungen und bei der Formulierung von funktionalen Spezifikationen für TOE (EVG)	Vorgeschriebene Darlegung zu den Evaluationskriterien bei der Feststellung, ob ein TOE (EVG) die postulierten Sicherheitsfunktionen wirksam erreicht
Teil 3 Vertrauenswürdigkeitsanforderungen	Anleitung bei der Festlegung der erforderlichen Vertrauenswürdigkeitsstudien	Nachschlagewerk bei der Interpretation von Darlegungen von Anforderungen an die Vertrauenswürdigkeit und bei der Feststellung der Herangehensweise an die Vertrauenswürdigkeit von TOE (EVG)	Vorgeschriebene Darlegung zu den Evaluationskriterien bei der Feststellung, der Vertrauenswürdigkeit von TOE (EVG) und bei der Prüfung und Bewertung von PP und ST.

Vergleich von Protection Profile (PP) gegenüber Security Target (ST)

Das *Protection Profile (Schutzprofil)* stellt eine implementierungsunabhängige Menge von Sicherheitsanforderungen dar, die auf eine ganze Produkt (=TOE-) Familie anwendbar sind, z. B. Firewalls, Betriebssysteme, Chipkarten.
Demgegenüber sind *Security Targets (Sicherheitsvorgaben)* implementierungsabhängig und stellen somit ein erweitertes PP dar, falls ein geeignetes (bzw. registriertes) PP vorhanden ist.

Granularität der Sicherheitsanforderungen (funktional)

Durch einen hierarchischen Aufbau der Sicherheitsanforderungen soll einem Anwender der CC das Auffinden einzelner Anforderungen erleichtert werden. Hierbei ist die Klasse die allgemeinste Gruppierung von Sicherheitsanforderungen, ihr folgen Familie, Komponente und Element mit ansteigendem Detaillierungsgrad.



Quelle: BSI, CC Version 2.1, 1999

Nachfolgend soll beispielhaft der Weg der Recherche zu einer spezifischen Sicherheitsanforderung gezeigt werden. Die Suche beginnt bei den Funktionalitätsklassen:

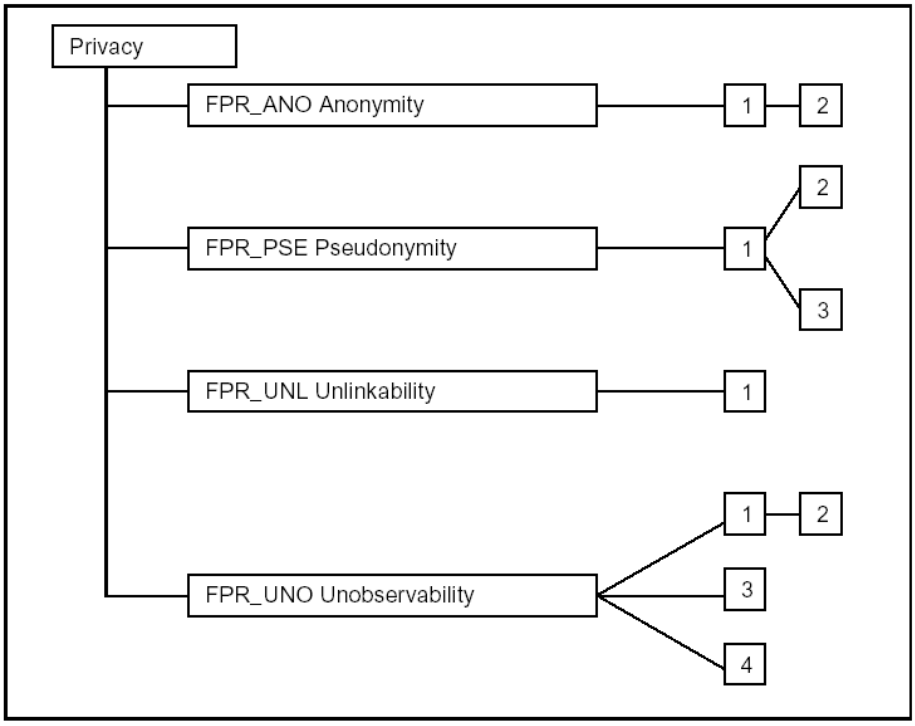
– FAU (Sicherheitsprotokollierung)
– FAU (Sicherheitsprotokollierung)
– FCO (Kommunikation)
– FCS (Kryptographische Unterstützung)
– FDP (Schutz der Benutzerdaten)
– FIA (Identifikation und Authentisierung)
– FMT (Sicherheitsmanagement)
– FPR (Privatsphäre)
– FPT (Schutz der EVG- Sicherheitsfunktionen)
– FRU (Betriebsmittelnutzung)
– FTA (EVG- Zugriff)
– FTP (vertrauenswürdiger Pfad/ Kanal)

Hat man festgestellt, daß in die gesuchte Funktionalität in einer Klasse vorhanden ist, untersucht man diese genauer:

Beispiel: Klasse FPR (Privatsphäre) mit ihren Familien

- Anonymität (FPR_ ANO) des Benutzers
- Pseudonymität (FPR_ PSE) des Benutzers
- Unverkettbarkeit (FPR_ UNL) der Benutzeraktionen
- Unbeobachtbarkeit (FPR_ UNO) der Benutzeraktionen

Dieser Vorgang wird solange wiederholt, bis man "passende" Sicherheitselemente ermitteln kann.



Quelle: BSI, Common Criteria, Version 2.1 (1999)

Wird ein adäquates Element nicht gefunden, ist eine Definition neuer Elemente notwendig.

Eine solche Zusammenstellung von "Übersetzungen" des bisherigen Anforderungskataloges ist im Kapitel III beispielhaft erfolgt.

Vertrauenswürdigkeitsanforderungen

Die im dritten Teil der Common Criteria definierten Vertrauenswürdigkeitsanforderungen werden analog zu den Funktionalitätsanforderungen in Klassen, Familien, Komponenten und Elemente strukturiert.

Nachstehend wird beispielhaft diese Struktur wiedergegeben:

Vertrauenswürdigkeits*klassen*

- Konfigurationsmanagement (ACM)
- Auslieferung und Betrieb (ADO)
- Entwicklung (ADV)
- Handbücher (AGD)
- Lebenszyklus- Unterstützung (ALC)
- Testen (ATE)
- Schwachstellenbewertung (AVA)
- Erhalten der Vertrauenswürdigkeit (AMA)
- Prüfung und Bewertung des Schutzprofils (APE)
- Prüfung und Bewertung der Sicherheitsvorgaben (ASE)

Vertrauenswürdigkeits*familien*

•Beispiel:
– Klasse AVA (Schwachstellenbewertung)
• Familien:
– AVA_ CCA: Analyse der verdeckten Kanäle
– AVA_ MSU: Missbrauch
– AVA_ VLA: Stärke der EVG- Sicherheitsfunktionen und Schwachstellenanalyse

Vertrauenswürdigkeits*komponenten*

•Beispiel:
– Klasse AVA (Schwachstellenbewertung)
• Familien:
– ...
– AVA_ MSU: Missbrauch
Komponenten:
» AVA_ MSU. 1 Prüfung der Handbücher
» AVA_ MSU. 2 Gültigkeit der Analyse
» AVA_ MSU. 3 Analysieren und Testen auf unsichere Zustände

Die Ableitung der "**Vertrauenswürdigkeitsstufen**" – also „Pakete von Vertrauenswürdigkeitskomponenten“ erfolgt nach der folgenden Wertung:
– EAL1 (funktionell getestet)
– EAL2 (methodisch getestet und überprüft)
– EAL3 (methodisch getestet und überprüft)
– EAL4 (methodisch entwickelt, getestet und durchgesehen)
– EAL5 (semiformal entworfen und getestet)
– EAL6 (semiformal verifizierter Entwurf und getestet)
– EAL7 (formal verifizierter Entwurf und getestet)

Der bei Prüfungen im Rahmen des Datenschutz-Gütesiegels zunächst anzustrebende Evaluierungslevel sollte bei EAL1 bzw. EAL2 liegen.