Prüfschema des Gutachtens für die Produktzertifizierung
Version 2.0 vom 17.06.2015[1]

I. Allgemeiner Teil

Im Folgenden wird das Prüfschema für Gutachten dargestellt, nach dem bei der Produktzertifizierung nach der DSGSVO vorzugehen ist. Im ersten Teil des Prüfschemas muss ein Formular zum IT-Produkt und zu der Prüfung ausgefüllt werden. Der zweite Teil besteht aus einer Anleitung, wie die Sachverständigen das IT-Produkt auf die Erfüllung der datenschutzrechtlichen Vorschriften prüfen.
Feldüberschriften sind dann kursiv gesetzt, wenn ihr Inhalt – ggf. gekürzt – ins Kurzgutachten[2] übernommen wird.

Zeitpunkt der Prüfung

Adresse des Antragstellers[3]

Adressen des/der Sachverständigen[4]

[1] **Historie:** V 1.0 (01.02.2002): Erstellung // V 1.0a (21.02.2002): Korrektur // V 1.1 (01.11.2005): Anpassung an Anforderungskatalog // V 2.0 (11.06.2015): Anpassung an Anforderungskatalog 2.0.
[2] Zusammenfassung der Prüfung zum Zweck der Veröffentlichung durch das Unabhängige Landeszentrum für Datenschutz nach § 2 Abs. 2 Nr. 6 DSGSVO.
[3] Vollständige Kontaktadresse mit Ansprechpartner.
[4] Vollständige Kontaktadresse mit Ansprechpartnern.

Kurzbezeichnung des IT-Produktes

Detaillierte Bezeichnung des IT-Produktes[5]

[5] Mit der detaillierten Bezeichnung des IT-Produktes wird der Prüfgegenstand festgelegt. Dazu gehört auch die Darstellung von Einsatzbedingungen (z. B. zugrundeliegende Betriebssysteme, ggf. nötige Zusatzprogramme inkl. Versionsnummer, notwendige Konfiguration für den datenschutzgerechten Einsatz etc.), von Grenzen des IT-Produktes oder von Schnittstellen zu nicht unmittelbar im Produkt enthaltenen Funktionen oder Modulen. Bei der Beschreibung von enthaltenen oder ggf. zum Betrieb notwendigen Komponenten sollen sich die Sachverständigen an der Komponentenliste in Abschnitt VI orientieren.

Tools, die zur Herstellung des IT-Produktes verwendet wurden[6]

Zweck und Einsatzbereich[7]

[6] Die Angabe der Tools, die zur Herstellung des Produktes verwendet wurden, ist zurzeit freiwillig. Das ULD begrüßt dies allerdings, und ggf. können durch diese Angabe Rückfragen vermieden werden. Bei der Nennung sollen sich die Sachverständigen an der Komponentenliste in Abschnitt VI orientieren (s. a. vorige Fußnote).

[7] Durch Zweck und Einsatzbereich bestimmen sich die Rechtsgrundlagen, die für das Anforderungsprofil an das Produkt heranzuziehen sind. Je enger Zweck und Einsatzbereich gefasst sind, desto kürzer wird in der Regel die Prüfung, da sie sich auf die einschlägigen Rechtsgrundlagen beschränkt. Bei einer weiten Fassung von Zweck und Einsatzbereich müssen häufig sehr viel mehr rechtliche Anforderungen überprüft werden. Man kann sich auch auf nicht-sensible Daten beschränken, die mit dem zu zertifizierenden Produkt zu verarbeiten sein sollen. Zu den sensiblen Daten gehören insbesondere solche, die einer beruflichen Schweigepflicht unterfallen sowie die in Art. 8 EU-Datenschutzrichtlinie bzw. § 11 Abs. 3 LDSG aufgeführten Daten.
Unter **"Zweck"** sind die Verarbeitungszwecke im Hinblick auf die Funktionalität der Datenverarbeitungsvorgänge des IT-Produktes anzugeben. Beispiel: "Adressverwaltung".
Im Gegensatz zu der im Datenschutzrecht verwendeten Zweckbindung bezieht sich diese auf die beabsichtigte Zielsetzung der Datenverarbeitung für den konkreten Einsatz und ist daher in der Regel spezieller auf Einzelfälle der Datenverarbeitungsprozesse bezogen.
Der **"Einsatzbereich"** beschreibt, für welche Geschäftsbereiche (personell, organisatorisch, institutionell) das IT-Produkt zertifiziert werden soll. Hier können sowohl Einsatzbereiche aufgezählt als auch bestimmte Einsatzbereich explizit ausgenommen werden.

Modellierung des Datenflusses[8]

Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Angewandte Evaluationsmethoden

[8] An dieser Stelle ist eine übersichtsartige Zerlegung des Produktes in Komponenten und Modellierung des Datenflusses anzugeben. Insbesondere ist eine Kennzeichnung wichtig, ob und welche Datenarten besonders kritisch oder sensibel sind. Diese Darstellung ist hilfreich, um die einschlägigen Rechtsgrundlagen für die verarbeiteten Datenarten zu finden und zu benennen. Im Anhang wird dies anhand eines Beispiels gezeigt.

Zusammenfassung der Prüfungsergebnisse

Sofern das Produkt einen Teil der Anforderungen nur unzureichend erfüllt: Beschreibung, wie dies ausgeglichen wird[9]

[9] Siehe III.5.2: Die wertende Gesamtbetrachtung muss die Vereinbarkeit mit den Vorschriften im Sinne von § 2 Abs. 2 Satz 1 Nr. 4 DSGSVO ergeben.

Beschreibung, wie das IT-Produkt den Datenschutz fördert[10]

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht. Die ausführliche Analyse liegt bei.

Ort, Datum Unterschriften der Sachverständigen

Beizufügende Unterlagen:

- Ausführliche Darstellung der Prüfung mit Analyse und Bewertung, ob das IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht
- Erklärung zur Unabhängigkeit des/der Sachverständigen bzw. durch Leiter der Prüfstelle

[10] In dieser Rubrik soll beschrieben werden, mit welchen Funktionen oder Konzepten das Produkt besonders datenschutzfördernd wirkt oder Innovationen im Datenschutz- oder Datensicherheitsbereich aufweist.

II. Vorgehen zur Analyse, ob das IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht:

Nach § 2 Abs. 2 Nr. 4 und 5 DSGSVO müssen im Gutachten die folgenden Angaben gemacht werden:

- besondere Eigenschaften des IT-Produktes, insbesondere zur Datenvermeidung und Datensparsamkeit (§ 4 Abs. 1 und § 11 Abs. 4 und 6 LDSG), Datensicherheit, Beachtung der Schutzziele und Revisionsfähigkeit der Datenverarbeitung (§§ 5 und 6 LDSG), Gewährleistung der Rechte der Betroffenen (§§ 26 bis 30 LDSG)
- Bewertung der besonderen Eigenschaften

Unter "besondere Eigenschaften" werden hier alle Funktionalitäten des IT-Produktes verstanden, die von den für den jeweiligen Zweck und Einsatzbereich einschlägigen Rechtsvorschriften über den Datenschutz und die Datensicherheit umfasst werden.

Bei der Prüfung wird schrittweise vorgegangen:

1. Zunächst werden die unterschiedlichen **Datenarten**, die im IT-Produkt eine Rolle spielen, identifiziert (s. a. Abschnitt "Modellierung). Man unterscheidet
   - Primärdaten, auf deren Datenverarbeitung das IT-Produkt vornehmlich abzielt (z. B. Betroffenendaten, Inhaltsdaten), und
   - Sekundärdaten, die aus unterschiedlichen Gründen zusätzlich bei der Datenverarbeitung anfallen (z. B. Nutzungsdaten, Zahlungsabwicklungsdaten, Protokolldaten, Statistikdaten, Autorisierungsdaten).

   Das erforderliche Schutzniveau kann sich für die Datenarten erheblich unterscheiden.

2. Ausgehend von den verschiedenen Datenarten werden jeweils aus den für die entsprechenden Daten und Anwendungszusammenhänge (Zweck und Einsatzbereich) einschlägigen Rechtsvorschriften über den Datenschutz und die Datensicherheit **Anforderungsprofile** erstellt. Dazu werden **pro Datenart**
   - alle einschlägigen Rechtsnormen über Datenschutz und Datensicherheit aufgeführt,
   - aus diesen Rechtsnormen jeweils Teil-Anforderungsprofile erstellt sowie
   - diese Teil-Anforderungsprofile unter Berücksichtigung von Vorrangregeln zu einem Datenart-Anforderungsprofil (DAP) zusammengeführt.

   Alle Datenart-Anforderungsprofile bilden ein (Gesamt-)Anforderungsprofil für das Produkt. Aus Gründen der Nachvollziehbarkeit müssen sowohl die als einschlägig identifizierten Rechtsnormen als auch die DAP je Datenart im Gutachten dargestellt werden. Zumindest in Zweifelsfällen sollten die Entscheidungen für oder gegen die Einschlägigkeit oder den Vorrang einer Rechtsnorm ebenfalls dokumentiert werden. Die DAP beinhalten sowohl "positive Anforderungen", bei denen Funktionalität im IT-Produkt vorhanden sein muss, um sie zu erfüllen, als auch "negative

Anforderungen", bei denen bestimmte Funktionalität eben nicht beim IT-Produkt auftreten darf.

3. Diese DAP stellen das Soll dar, gegen die die Ist-Funktionalität des IT-Produktes **abzugleichen** ist:

   - Als erstes soll die Produktbeschreibung, die Bestandteil des IT-Produktes ist und eine Produktdokumentation, Hinweise auf die Einsatzbedingungen sowie einen Beipackzettel (Datenschutzhinweisblatt) enthält, daraufhin untersucht werden, ob sie tatsächlich wahrheitsgemäß das Produkt beschreibt. Ist dies nicht der Fall, kann kein Gütesiegel erteilt werden.
   - Für jede Anforderung und schließlich für das gesamte DAP wird (je Datenart) geprüft, ob das IT-Produkt samt der Produktbeschreibung die geforderte Funktionalität erfüllt.

   Bewertungskriterien sind der Stand der Technik (ist der Grad der technischen Umsetzung angemessen?), der notwendige Aufwand zur Realisierung des datenschutzgerechten Einsatzes sowie die Nutzeradäquanz. Die "Hinweise zur Bewertung" im nächsten Abschnitt geben Aufschluss über die verschiedenen Bewertungsmöglichkeiten: "Das Produkt entspricht der Anforderung *in vorbildlicher Weise / in adäquater Weise / in unzureichender Weise / nicht*."

   Es sind im Gutachten zu dokumentieren:

   - die Einzelbewertungen pro Anforderung,
   - die Bewertung pro DAP (je Datenart) und
   - die Gesamtbewertung über das gesamte Anforderungsprofil (die DAP aller Datenarten).

   Jede Bewertung muss begründet werden. Sofern von der Möglichkeit des Ausgleichens von Unzulänglichkeiten des IT-Produktes Gebrauch gemacht werden soll oder bestimmte Anforderungen im Einzelfall nicht betrachtet werden sollen, ist dies besonders zu belegen.

Es ist stets auf die Schlüssigkeit des Gutachtens zu achten, damit das ULD die Ergebnisse nachvollziehen und das IT-Produkt zertifizieren kann.

III. Hinweise zur Bewertung

Hinweise zur Bewertung für die Vergabe des Gütesiegels

1. Das Gütesiegel wird an IT-Produkte vergeben, die mit den Vorschriften über den Datenschutz und die Datensicherheit vereinbar sind.

2. Es wird bewertet, ob die Vereinbarkeit mit den Vorschriften aufgrund der besonderen Eigenschaften, die das Produkt aufweisen muss, vorliegt (§ 2 Abs. 2 Satz 1 Nr. 4 DSGSVO).

3. Besondere Eigenschaften sind die datenschutzrelevanten Eigenschaften. Für jedes Produkt wird festgestellt, welche Eigenschaften datenschutzrelevant sind. Dazu werden die an das jeweilige Produkt zu stellenden Anforderungen aus Zweck und Einsatzbereich und unter Berücksichtigung des Standes der Technik ermittelt. Die Gesamtheit der Anforderungen, die jeweils für ein Produkt ermittelt werden, wird als Anforderungsprofil bezeichnet.

4. Bei der Bewertung der besonderen Eigenschaften (§ 2 Abs. 2 Nr. 5 DSGSVO) wird festgestellt, ob das Produkt den einzelnen Anforderungen entspricht. Dabei erfolgt eine Zuordnung des Produktes zu einer der folgenden Kategorien:

   4.1. Das Produkt entspricht der Anforderung in vorbildlicher Weise. Dies ist der Fall, wenn die verwendeten technischen Lösungen in besonderer oder innovativer Weise die Ziele des Datenschutzes und der Datensicherheit fördern.

   4.2. Das Produkt entspricht der Anforderung in adäquater Weise. Dies ist der Fall, wenn die verwendeten technischen Lösungen die Umsetzung der gesetzlichen Vorgaben ermöglichen.

   4.3. Das Produkt entspricht der Anforderung in unzureichender Weise. Dies ist der Fall, wenn die verwendeten technischen Lösungen die Umsetzung der gesetzlichen Vorgaben nur dann ermöglichen, wenn erhebliche zusätzliche technische und organisatorische Maßnahmen beim Einsatz des Produkts ergriffen werden und in einer Dokumentation die Grenzen der technischen Umsetzung sowie die erforderlichen zusätzlichen technischen und organisatorischen Maßnahmen nutzerfreundlich beschrieben werden.

   4.4. Das Produkt entspricht der Anforderung nicht. Dies ist der Fall, wenn

      4.4.1. die verwendeten technischen Lösungen die Umsetzung der gesetzlichen Vorgaben auch bei Ergreifen von zusätzlichen technischen und organisatorischen Maßnahmen nicht ermöglichen oder

      4.4.2. die zur Ermöglichung der Vorgaben zu ergreifenden zusätzlichen technischen und organisatorischen Maßnahmen einen unzumutbaren Aufwand erfordern würden oder

      4.4.3. die Grenzen der technischen Umsetzung nicht beschrieben wurden oder

4.4.4. die zusätzlichen technischen und organisatorischen Maßnahmen nicht nutzerfreundlich beschrieben wurden oder

4.4.5. eine falsche, lückenhafte oder irreführende Produktbeschreibung vorliegt oder datenschutzrelevante Funktionen risikobehaftet umgesetzt sind.

5. Das Gütesiegel wird für ein Produkt nach folgenden Maßgaben erteilt:

5.1. Das Gütesiegel wird erteilt, wenn das Produkt allen Anforderungen des Anforderungsprofils im Sinne von 4.1 und 4.2 in vorbildlicher oder in adäquater Weise entspricht.

5.2. Das Gütesiegel kann auch erteilt werden, wenn das Produkt nur einem Teil der Anforderungen des Anforderungsprofils im Sinne von 4.1 und 4.2 in vorbildlicher oder in adäquater Weise entspricht (d. h. andere Anforderungen werden nur unzureichend im Sinne von 4.3 erfüllt) und eine wertende Gesamtbetrachtung die Vereinbarkeit mit den Vorschriften im Sinne von § 2 Abs. 2 Satz 1 Nr. 4 DSGSVO ergibt. Für eine Vereinbarkeit mit den Vorschriften spricht es insbesondere, wenn das Produkt einer Anforderung oder mehreren Anforderungen des Anforderungsprofils in vorbildlicher Weise entspricht.

5.3. Das Gütesiegel wird nicht erteilt, wenn das Produkt einer Anforderung des Anforderungsprofils im Sinne von 4.4 nicht entspricht.

IV. Struktur für die Dokumentation des Anforderungsprofils und der einzelnen Bewertungen

Die folgende Struktur ist als Übersicht über das Gutachten zu verstehen, in dem alle einschlägigen Punkte später aufgegriffen und ausführlich abgearbeitet werden. Aus Gründen der Einheitlichkeit der Gutachten müssen die Sachverständigen sich an dieser Struktur orientieren.

Diese Tabellen sind für jede Datenart zu erstellen. Die Anforderungen ergeben sich aus den einschlägigen Rechtsgrundlagen. Beispielhaft für die großenteils einschlägigen Anforderungen im Anforderungskatalog sind die Tabellen bereits vorausgefüllt. Sofern genannte Punkte allerdings nicht einschlägig sind, ist dies im Kommentarfeld zu dokumentieren. Zusätzliche einschlägige Rechtsnormen sind zu ergänzen und in Einzelanforderungen aufzuführen (siehe freie Zeilen; zum Ausfüllen kann auch eine elektronische, weiter bearbeitbare Version dieses Dokuments verwendet werden).

Das Feld "Bewertung" enthält eine Bewertung je Anforderung, wie es im Abschnitt III erläutert wird, d.h. die Kennzeichnung "vorbildlich", "adäquat", "unzureichend", "nicht".

Im Kommentarfeld wird angegeben, wenn unzureichend erfüllte Anforderungen bestehen, die ausgeglichen werden sollen. Außerdem sollen hier die angelegten Rechtsgrundlagen dokumentiert werden. Ebenso ist hier anzugeben, wenn eine aufgeführte Anforderung für das IT-Produkt unter Berücksichtigung von Zweck und Einsatzbereich nicht einschlägig ist oder aus anderen Gründen nicht in die Gesamtbewertung einfließen soll. Da der Platz in dieser Übersichtsstruktur beschränkt ist, bieten sich Verweise auf den Langtext des Gutachtens an.

Zu beachten ist, dass die Tabelle zur besseren Übersicht dem Gutachten beizufügen ist. Sie kann nicht den Langtext des Gutachtens ersetzen, sondern nur zusammenfassen.

Datenart: _____

Anforderung nach Katalog oder sonstigen Rechtsnormen	**Bewertung**	**Kommentare**
Allgemeines Anforderungsprofil		
Komplex 1:		
1.1 IT-Sicherheits-Schutzziele: Verfügbarkeit, Integrität, Vertraulichkeit		
1.2 Datenschutz-Schutzziel: Nicht-Verkettbarkeit (inkl. Datensparsamkeit, Zweckbindung und Zwecktrennung)		
1.3 Datenschutz-Schutzziel: Transparenz (inkl. Produktbeschreibung)		
1.4 Datenschutz-Schutzziel: Intervenierbarkeit		
1.5 Anpassung des IT-Produkts		
1.6 Privacy by Default		
1.7 Sonstige Anforderungen (benennen)		
Komplex 2:		

2.1. Ermächtigungsgrundlage		
2.1.1 Gesetzliche Ermächtigung		
2.1.2 Einwilligung des Betroffenen		
2.1.3 Besonderheiten in den einzelnen Phasen der Datenverarbeitung		
2.1.3.1 Vorschriften über die Datenerhebung		
2.1.3.2 Vorschriften über die Übermittlung		
2.1.3.3 Löschung nach Wegfall der Erfordernis		
2.2 Einhaltung allgemeiner datenschutzrechtlicher Grundsätze und Pflichten		
2.2.1 Zweckbindung und Zweckänderung		
2.2.2 Erleichterung der Umsetzung des Trennungsgebots		
2.2.3 Gewährleistung der Datensicherheit		
2.3 Datenverarbeitung im Auftrag		
2.4 Voraussetzungen besonderer technischer Verfahren		
2.4.1 Gemeinsames Verfahren / Abrufverfahren		
2.4.2 Trennung der Verantwortlichkeiten		
2.4.3 Veröffentlichungen im Internet		
2.4.4 Weitere besondere technische Verfahren		
2.5 Sonstige Anforderungen (benennen)		
2.5.1 Unterstützung Pseudonymität / Pseudonymisieren		
Komplex 3:		
3.1 Einzelne technisch-organisatorische Maßnahmen		
3.1.1 Physikalische Sicherung		
3.1.2 Authentisierung		
3.1.3 Autorisierung		
3.1.4 Protokollierung		
3.1.5 Verschlüsselung und Signatur		
3.1.6 Pseudonymisierung		
3.1.7 Anonymisierung		
3.2 Allgemeine Pflicht		
3.2.1 Technisch-Organisatorische Maßnahmen		
3.2.1.1 Verfügbarkeit		
3.2.1.2 Integrität		
3.2.1.3 Vertraulichkeit		
3.2.1.4 Nicht-Verkettbarkeit		
3.2.1.5 Transparenz		
3.2.1.6 Intervenierbarkeit		
3.2.1.7 Protokollierung von Datenverarbeitungsvorgängen		
3.2.1.8 Test und Freigabe		
3.2.2 Erleichterung der Vorabkontrolle		
3.2.3 Erleichterung der Erstellung von Verfahrensverzeichnissen		
3.2.4 Benachrichtigungspflicht		
3.2.5 Unterstützung behördlicher Datenschutzbeauftragter		
3.3 Spezifische Pflichten		
3.3.1 Verschlüsselung		
3.3.2 Anonymisierung oder Pseudonymisierung		

3.3.3 Spezielle Anforderungen bei besonderem Technikeinsatz		
3.3.3.1 Mobile Datenverarbeitungssysteme		
3.3.3.2 Video-Überwachung und –Aufzeichnung		
3.3.3.3 Automatisierte Einzelentscheidungen		
3.3.3.4 Veröffentlichungen im Internet		
3.4 Pflichten nach DSVO		
3.5 Anforderungen bei Auftragsdatenverarbeitung		
3.6 Sonstige Anforderungen (benennen)		
Komplex 4:		
4.1 Aufklärung und Benachrichtigung		
4.2 Benachrichtigung des Betroffenen bei unrechtmäßiger Kenntniserlangung von Daten		
4.3 Auskunft		
4.4.1 Berichtigung		
4.4.2 Vollständige Löschung		
4.4.3 Sperrung		
4.4.4 Einwand bzw. Widerspruch gegen die Verarbeitung		
4.4.5 Gegendarstellung		
4.5 Sonstige Anforderungen (benennen)		

B. Anforderungsprofil für Protokolldaten		
Komplex 1:		
1.1. Datenvermeidung und Datensparsamkeit		
1.2 Zweckbindung		
1.3 Nicht-Verkettbarkeit		
1.4 Transparenz		
1.5 Sonstige Anforderungen (benennen)		
Komplex 2:		
2.1 Rechtsgrundlage für die Erhebung und Verarbeitung der Protokolldaten		
2.2 Unterstützung der Einhaltung der Zweckbindung		
2.3 Aufbewahrungsfristen und Löschung		
2.4 Sonstige Anforderungen (benennen)		
Komplex 3:		
3.1 Fragestellungen aus 3.1.1		
3.2 Zugriffsschutz für Protokolldaten		
3.3 Informationsgehalt der Protokolldaten		
3.4 Einhaltung der Vorgaben des § 6 Abs. 4 LDSG (insbes. können Protokolldaten zusammen mit den gespeicherten Daten sichtbar gemacht werden?)		
3.5 Unterschiedliche Speicherfristen		
3.6 Verhinderung der unzulässigen Verkettung von Protokolldaten		
3.7 Maßnahmen beschrieben		
3.8 Sonstige Anforderungen (benennen)		
Komplex 4:		
4.1 Selektive Löschung von Einzeldaten		
4.2 Beauskunftung		
4.3 Berichtigung		
4.4 Sperrung		
4.5 Einwand		

V. Rückmeldung

Die Sachverständigen haben die Möglichkeit, dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein ihre Erfahrungen mit dem vorgegebenen Prüfverfahren rückzumelden und Anregungen für Verbesserungen zu geben:

Rückmeldung und Verbesserungsvorschläge
zu dem vom ULD vorgegebenen Prüfverfahren

VI. Liste von typischen Komponenten, die innerhalb von IT-Produkten zum Einsatz kommen können

Im Gutachten muss pro IT-Produkt bzw. pro Modul aufgeführt werden, welche Hard- und Software (in bestimmten Fällen auch welche Algorithmen oder Protokolle) zugrunde liegen oder die (datenschutzrechtlich relevante) Funktionalität des Produktes beeinflussen können. Diese Informationen werden beim ULD erfasst. Bei Bekanntwerden von relevanten Fehlern oder konkreten Sicherheitsvorkommnissen, die im Zusammenhang mit dem zertifizierten Untersuchungsgegenstand stehen, kann das ULD die Hersteller/Vertriebsfirmen zur Klärung des Sachverhalts und ggf. zur Nachbesserung und erneuter Begutachtung auffordern.

Die Liste ist nicht vollständig und wird ständig erweitert. Sie dient den Sachverständigen zur Orientierung bei der Angabe der Komponenten im Zusammenhang mit dem IT-Produkt. Die dargestellte Gruppierung soll das Auffinden von Komponenten erleichtern, ist aber aufgrund der vielfältigen Funktionalitätsüberschneidungen der Komponenten nicht schnittmengenfrei.
Pro Komponente, die in diesem Fall Hardware, Software, Algorithmen und Protokolle umfasst, ist alles anzugeben, was zu ihrer eindeutigen Identifizierung notwendig ist:

- Name,
- Hersteller,
- Typ,
- Versionsnummer,
- ggf. Datum des Releases,
- ggf. Zertifikate anderer Prüfstellen
- ggf. weitere relevante Hinweise oder Bemerkungen, z. B. wiederum Informationen zu deren Herstellungstools.

Beispiel:

MeinProdukt, Version 3.4 enthält bzw. verwendet folgende wesentliche Komponenten:

- Virenschutzprogramm *AntiVirenProgramm*, Firma *Antivirus GmbH*, Meinfurt, Version v 1.4 vom 1.1.2002 mit halbautomatisierten Updates der Virendefinition.
- Chipkartenleser *MyChipCard,* Firma *KryptoProdukte AG*, Meinburg, Typ *Card 2002*, Version 1.1, mit Tastatur, zertifiziert vom BSI 2001, Zertifikatsnummer BSI-CC-0001-2001.
- SDK *Chipware für MyChipCard Card 2002,* Firma *KryptoProdukte AG*, Meinburg, Version v 2.4, Bibliotheken für C++ und Java.
- Verschlüsselungsalgorithmen *MyCryptoLibrary*, Firma *CryptoProducts* Inc., MyPolis (USA), Version 2.4, Bibliotheken für C++ und Java. Dies Produkt baut auf der Kryptobibliothek CRYPT in der Version 2.7.3 (2000) auf. Genutzt werden die Algorithmen *IDEA* und *Blowfish*, mit einer Schlüssellänge von 128 Bit im CBC-Modus (IDEA) und 448 Bit

(Blowfish). Als Hashverfahren kommt *SHA-1* zum Einsatz.

- Herstellungswerkzeuge: GNU C-Compiler gcc, Version 3.0.1; GNU Java Compiler GJC 3.0.2 mit der Bibliothek libgjc.