Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten[1]

- Arbeitsgrundlage für Entwickler/Hersteller und Prüf-/Bestätigungsstellen -

1. Vorbemerkungen und Zielsetzung

Bei Signaturprodukten mit gesetzlichem Gütezeichen wird die Erfüllung der Anforderungen nach Signaturgesetz und Signaturverordnung durch gesetzlich anerkannte Stellen vorab überprüft und bestätigt (vgl. § 15 Abs. 7 Satz 1 Signaturgesetz).

In der Sicherheitsbestätigung für ein Signaturprodukt ist auch anzugeben, unter welchen Einsatzbedingungen die Bestätigung gilt (vgl. Anlage 1 Nr. 3 Buchst. a) Signaturverordnung).

Die Einsatzbedingungen sind vor allem bei Signaturanwendungskomponenten von Bedeutung, da die durch Signaturgesetz/Signaturverordnung vorgegebene hohe Sicherheit bei diesen unter bestimmten Einsatzbedingungen einfacher und preiswerter erreicht werden kann. Andererseits machen restriktive Einsatzbedingungen Signaturprodukte weniger attraktiv.

Mit diesem Dokument wird ein Rahmen für eine einheitliche Spezifizierung der Einsatzbedingungen in den Sicherheitsbestätigungen vorgegeben[2] (einheitliche Strukturierung der unterschiedlichen Einsatzbereiche/spezifischen Einsatzbedingungen).
Es hat zum ***Ziel***,

- vorrangig ***konstruktive Sicherheitslösungen*** zu erreichen und die Einsatzbedingungen auf ein Mindestmaß zu begrenzen,
- erforderliche ***Einsatzbedingungen*** für alle Beteiligten (Hersteller/Vertreiber, Prüf-/Bestätigungsstellen nach § 18 Signaturgesetz und Betreiber/Nutzer) ***transparent*** zu ***machen***,
- über ein online abrufbares Verzeichnis der Regulierungsbehörde**,** das alle (nach einheitlicher Struktur gestalteten) Sicherheitsbestätigungen enthält, einen ***Vergleich der Produkte*** bezüglich der Einsatzbedingungen zu erleichtern (dies dient der Förderung von Produkten, die auch ohne restriktive Einsatzbedingungen hohe Sicherheit bieten), und
- zu gewährleisten, dass nur ***praxisgerechte Einsatzbedingungen*** gestellt werden und dass die Betreiber/Nutzer von Signaturanwendungskomponenten ***geeignete Bedienungsanweisungen*** erhalten, an Hand derer sie sicher erkennen können, welche Einsatzbedingungen sie zu beachten haben[3].

Zum besseren Verständnis werden zunächst die Sicherheitsanforderungen an Signaturanwendungskomponenten nach Signaturgesetz und Signaturverordnung vorangestellt.

2. Sicherheitsanforderungen an Signaturanwendungskomponenten[4]

2.1 Erzeugung von Signaturen

Die Signaturanwendungskomponente muss beim Erzeugen einer Signatur gewährleisten, dass

- das Erzeugen einer ***Signatur*** vorher eindeutig ***angezeigt*** wird[5]**,**
- ***erkennbar*** ist, auf ***welche Daten*** sich die Signatur bezieht[6],
- ***bei Bedarf*** der ***Inhalt*** der zu signierenden Daten hinreichend zu ***erkennen*** ist[7],
- eine ***Signatur nur durch*** die ***berechtigt signierende Person*** erfolgt[8],
- die ***Identifikationsdaten nicht preisgegeben*** und nur auf der jeweiligen „sicheren Signaturerstellungseinheit“ gespeichert werden[9].

2.2 Prüfung einer Signatur
Die Signaturanwendungskomponente muss beim Prüfen einer Signatur gewährleisten, dass

- erkennbar wird, ***auf welche Daten*** sich die Signatur bezieht,
- erkennbar wird, ob die ***Daten unverändert*** sind,
- bei Bedarf der ***Inhalt der signierten Daten*** hinreichend zu erkennen ist,
- erkennbar wird, welchem ***Signaturschlüssel-Inhaber*** die Signatur zuzuordnen ist,
- erkennbar wird, welche ***Inhalte*** das ***qualifizierte Zertifikat***, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen,
- erkennbar wird, ob die nachgeprüften qualifizierten ***Zertifikate*** im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt ***vorhanden und nicht gesperrt*** waren,
- die ***Korrektheit der Signatur*** zuverlässig geprüft und ***zutreffend angezeigt*** wird.

2.3 Schutz vor unbefugter Veränderung
Sicherheitstechnische Veränderungen an der Signaturanwendungskomponente müssen für den Nutzer erkennbar [10]werden**.**

2.4 Stärke der Sicherheitsmechanismen und Prüfstufe
Die zur Erfüllung der Anforderungen nach den Abschnitten 2.1 bis 2.3 eingesetzten Sicherheitsmechanismen müssen ausnahmslos die Stärke „hoch[11]**“** aufweisen und mindestens nach der Prüfstufe „E 2“ gemäß den ITSEC oder „EAL 3+[12]“ gemäß den Common Criteria geprüft und bestätigt sein [13](vgl. Anlage 1 Nr. 1 Signaturverordnung).

3. Potentielle Bedrohungen
Die vorgegebene hohe Sicherheit für Signaturanwendungskomponenten (Abschnitt 2.4) ist potentiell bedroht [14]durch

- Angriffe über Kommunikationsnetze[15],
- Angriffe über manuellen Zugriff Unbefugter/Datenaustausch per Datenträger[16] und
- Fehler/Manipulationen bei Installation, Betrieb/Nutzung und Wartung/Reparatur.

4. Unterschiedlicher „Mix“ von Sicherheitsvorkehrungen
Den potentiellen Bedrohungen kann durch einen unterschiedlichen „Mix“ von Sicherheitsvorkehrungen in der

- Signaturanwendungskomponente selbst und
- Einsatzumgebung

begegnet werden (siehe Anlagen 1 und 2).

Um zu bedarfsgerechten technischen Lösungen zu gelangen, sind konzeptionell folgende Einsatzbereiche zu unterscheiden:

4.1 Ungeschützter Einsatzbereich (*Sonderfall/spezielle Lösung)*
Die Signaturanwendungskomponente wird in einer „Signatur-Arbeitstation“

- mit ***ungesicherter Anbindung*** an das ***Internet*** und
- ***ohne*** signaturspezifische ***Sicherheitsvorkehrungen in der Einsatzumgebung*** (gegen Bedrohungen über Internet/Intranet und manuellen Zugriff Unbefugter/Datenaustausch per Datenträger)

eingesetzt [17].

4.2 Geschützter Einsatzbereich (*Regelfall/Standardlösung)*
Die Signaturanwendungskomponente wird in einer „Signatur-Arbeitsstation“ eingesetzt, bei der gegenüber den potentiellen Bedrohungen folgender Schutz besteht[18]:
Potentielle Angriffe über

- das Internet,
- ein angeschlossenes Intranet,
- einen manuellen Zugriff Unbefugter und
- Datenaustausch per Datenträger

werden durch eine ***Kombination von Sicherheitsvorkehrungen*** in der Signaturanwendungskomponente selbst und der Einsatzumgebung mit hoher Sicherheit ***abgewehrt***.

4.3 Isolierter Einsatzbereich *(Sonderfall/spezielle Lösung)*
Die Signaturanwendungskomponente wird in einer „Signatur-Arbeitsstation“ eingesetzt, bei der gegenüber den potentiellen Bedrohungen folgender Schutz besteht[19]:

- Es erfolgt ***zu keinem Zeitpunkt*** eine ***Anbindung an*** ein ***Kommunikationsnetz***[20] und
- in der ***Einsatzumgebung*** sind ***Sicherheitsvorkehrungen*** vorhanden, die potentielle Angriffe über manuellen Zugriff Unbefugter/Datenaustausch per Datenträger mit hoher Sicherheit abwehren[21].

5. Sicherheitsbestätigung
Bei der ***Bestätigung der Sicherheit*** einer Signaturanwendungskomponente ist ***anzugeben***,

- für welche der o.a. ***Einsatzbereiche***[22] die Signaturanwendungskomponente geeignet ist,
- unter welchen ***Einsatzbedingungen*** das Produkt die vorgegebene hohe Sicherheit dort aufweist und
- wie der Betreiber/Nutzer zuverlässig ***erkennen*** kann, dass ***das Produkt*** sich ***in sicherem Zustand*** befindet

Neben **produktspezifischen** sind als **generelle Einsatzbedingungen** (für alle Einsatzbereiche) in jeder Sicherheitsbestätigung zu benennen:

- Eine ***geeignete Bedienungsanweisung***, die in allgemein verständlicher Sprache gehalten ist und potentiellen sicherheitsrelevanten Fehlern beim Betrieb/der Nutzung des Produktes ***praxisgerecht*** hinreichend vorbeugt.

  Sie muss eine präzise Beschreibung aller Einsatzbedingungen (von der Installation über Betrieb/Nutzung bis zur Wartung/Reparatur) enthalten, die eingehalten werden müssen, um die vorgegebene hohe Sicherheit zu gewährleisten.

  Sie soll darüber hinaus auch ausdrücklich auf typische sicherheitsrelevante Fehler bei Betrieb/Nutzung der Signaturanwendungskomponente (z.B. unbeaufsichtigte „Signatur-Arbeitsstation“ mit scharf geschaltetem Signaturschlüssel, gemeinsame Aufbewahrung von Signaturerstellungseinheit und PIN oder Wartung/Reparatur der Signaturanwendungskomponente durch nicht autorisiertes Personal) sowie die potentiellen Risiken bei geschäftsmäßiger Nutzung ***fremder*** Signaturanwendungskomponenten hinweisen.

Der Hersteller/Vertreiber einer Signaturanwendungskomponente ist mit Ausstellung der Sicherheitsbestätigung ausdrücklich zu verpflichten, eine Beschreibung

- der Einsatzbereiche, für welche die Signaturanwendungskomponente geeignet ist, und
- aller Einsatzbedingungen

in geeigneter Weise (d.h. ohne inhaltliche Veränderung gegenüber der Sicherheitsbestätigung, aber unter möglicher Berücksichtigung von didaktischen und Marketingaspekten) in die Bedienungsanweisung aufzunehmen. Die Eignung der Bedienungsanweisung unter signaturspezifischen Sicherheitsaspekten ist Teil der Sicherheitsbestätigung.

- Eine ***sichere Wartung/Reparatur***, d.h.
  - das Wartungs-/Reparaturpersonal ist qualifiziert/vertrauenswürdig und ggf. vom Hersteller/Vertreiber autorisiert,
  - nach Wartung/Reparatur erfolgt eine Sicherheitsprüfung des Produkts und
  - sicherheitsgeprüfte Produkte werden bedarfsgemäß sicher aufbewahrt/transportiert.

Die **Einsatzbedingungen** sind in den Sicherheitsbestätigungen **nach einheitlichem Muster** entsprechend Anlage 2 zu **spezifizieren**.

Die Einsatzbedingungen müssen **praxisgerecht**, d.h. von einem durchschnittlichen Betreiber/Nutzer zu verstehen und mit zumutbarem Aufwand umzusetzen sein.

6. Gesetzliches Gütezeichen für Produkte

Das gesetzliche Gütezeichen nach § 15 Abs. 7 Signaturgesetz wird nur für Signaturanwendungskomponenten vergeben, deren Einsatzbedingungen nach vorstehenden Vorgaben spezifiziert wurden, und nur für vollständige Produkte gemäß § 2 Nr. 11 Buchst. a) und/oder b) Signaturgesetz.
Teilkomponenten (z.B. Chipkartenleser) können lediglich eine Sicherheitsbestätigung erhalten. Damit soll der Gefahr vorgebeugt werden, dass Betreiber/ Nutzer selbst aus Teilkomponenten ein (ggf. fragwürdiges) Gesamtprodukt konstruieren.

7. Verantwortung, Transparenz und Fortentwicklung

Die Verantwortung für den Inhalt dieses Dokumentes liegt bei der Regulierungsbehörde für Telekommunikation und Post. Es wurde in einem Workshop am 22.11.2001 mit Vertretern aus allen betroffenen Bereichen ausführlich diskutiert und danach mit den anerkannten Bestätigungsstellen nach § 18 Signaturgesetz abgestimmt.

Als zuständige Behörde nach dem Signaturgesetz obliegt der Regulierungsbehörde auch die Kontrolle, dass gemäß dem Papier verfahren wird.

Im Interesse einer optimalen Transparenz ist das Dokument über die Website der Regulierungsbehörde (http://www.regtp.de/elsig) online abrufbar, so dass es außer für die eigentlichen Adressaten (Entwickler/Hersteller und Prüf-/Bestätigungsstellen) auch für andere Interessierte (z.B. Wissenschaftler, Verbraucherschützer und Journalisten) verfügbar ist.

Das Dokument unterliegt insbesondere durch die Tätigkeit der anerkannten Prüf-/ Bestätigungsstellen einem fortwährenden Praxistest und wird bei Bedarf fortentwickelt. Anstöße dazu können auch von anderer Seite, etwa von den Produktherstellern, den Zertifizierungsdiensten oder dem Bundesverband der Verbraucherzentralen und Verbraucherverbände, kommen. Hierzu steht die E-Mail Adresse ElektronischeSignatur@regtp.de zur Verfügung.

Anlage 1

Komplettierung der Sicherheit gegenüber potentiellen Bedrohungen

Die vorgegebene hohe Sicherheit gegenüber potentiellen Angriffen wird in den verschiedenen Einsatzbereichen durch einen unterschiedlichen „Mix“ von Sicherheitsvorkehrungen wie folgt komplettiert[23]:

	Ungeschützter Einsatzbereich	**Geschützter Einsatzbereich**	**Isolierter Einsatzbereich**
Angriff aus dem Internet	Signaturanwendungs-komponente	Hohe Sicherheit durch Abschottung	Angriff nicht möglich
Angriff über das Intranet[24]	Signaturanwendungs-komponente	IT-Plattform, Signatur-anwendungs-komponente	Angriff nicht möglich
Angriff über manuellen Zugriff Unbefugter/Datenaustausch	Signaturanwendungs-komponente	Einsatzumgebung, IT-Plattform, Signatur-anwendungs-komponente	Hohe Sicherheit durch isolierten Einsatzbereich
Fehler/Manipulation bei Installation, Betrieb/Nutzung, Wartung/ Reparatur	Qualifiziertes/ vertrauenswürdiges Personal, administrative Sicherheitsmaßnahmen	Qualifiziertes/ vertrauenswürdiges Personal, administrative Sicherheitsmaßnahmen	Qualifiziertes/ vertrauenswürdiges Personal, administrative Sicherheitsmaßnahmen

Anlage 2

Spezifizierung der Einsatzbedingungen

Folgende Einsatzbedingungen sind zulässig/notwendig[26]:

„Lebenszyklus“ einer Signaturanwendungskomponente	Potentielle Einsatzbedingungen		
	Eignung für den ungeschützten Einsatzbereich	**Eignung für den geschützten Einsatzbereich**	**Eignung für den isolierten Einsatzbereich**
Einrichtung der „Signatur-Arbeitstation“			
Auflagen zur Anbindung an das Internet	Keine Auflagen	produktspezifische Auflagen[25]	Keine Anbindung an Internet
Auflagen zur Anbindung an ein Intranet	Keine Auflagen	produktspezifische Auflagen[25]	Keine Anbindung an Intranet
Auflagen zur Sicherheit der IT-Plattform und Applikationen	Keine Auflagen	Produktspezifische Auflagen	Keine Sicherheits- Beeinträchtigung [26]
Auflagen zur Auslieferung und Installation der Signaturanwendungskomponente	Keine Auflagen[27]	produktspezifische Auflagen	produktspezifische Auflagen
Maßnahmen in der Einsatzumgebung			
Auflagen zum Schutz vor manuellem Zugriff Unbefugter	Keine Auflagen	produktspezifische Auflagen[25]	Hoch sicher isoliert
Auflagen zum Schutz vor Angriffen über Datenaustausch per Datenträger	Keine Auflagen	produktspezifische Auflagen[25]	Datenüberprüfung auf Schadensprogramme[28]
Betrieb/Nutzung			
Auflagen zur Sicherheitsadministration des Betriebs	Keine Auflagen	produktspezifische Auflagen	produktspezifische Auflagen
Auflagen zum Schutz vor Fehlern bei Betrieb/Nutzung	geeignete Bedienungsanweisung	geeignete Bedienungsanweisung	geeignete Bedienungsanweisung
Wartung/Reparatur			
Anforderungen an das Wartungs-/Reparaturpersonal	qualifiziert/ vertrauenswürdig	qualifiziert/ vertrauenswürdig	qualifiziert/ vertrauenswürdig
Authentisierung des Personals	zuverlässige Authentisierung[29]	zuverlässige Authentisierung[29]	zuverlässige Authentisierung[29]
Aufbewahrung/Transport der Produkte	Keine Auflagen	geschützt vor unbemerktem manuellen Zugriff Unbefugter	geschützt vor unbemerktem manuellen Zugriff Unbefugter

Erläuterungen:

[1] Nach § 2 Nr. 11 Signaturgesetz vom 16.05.2001 (BGBl. I. S. 876) sind „Signaturanwendungskomponenten" Software- und Hardware-Produkte, die dazu bestimmt sind,

a) **Daten** dem **Prozess** der Erzeugung oder Prüfung **qualifizierter elektronischer Signaturen zuzuführen** oder

b) qualifizierte elektronische **Signaturen zu prüfen** oder qualifizierte Zertifikate nachzuprüfen und die **Ergebnisse anzuzeigen**.

Die **„Signaturanwendungskomponente" umfasst** somit die **gesamte Hard-/Software, mit der** die an diesen Begriff geknüpften **Anforderungen** nach Signaturgesetz und Signaturverordnung (siehe Abschnitte 2.1 und 2.2) **technisch umgesetzt werden**. Sie kann sich dabei verschiedener technischer Komponenten (z.B. Chipkartenleser und PC-Betriebssystem) bedienen.

[2] Absprache zwischen der Regulierungsbehörde für Post und Telekommunikation und den gesetzlich anerkannten Bestätigungsstellen (vgl. §18 Signaturgesetz). Sie findet ab dem **1. Februar 2002** Anwendung.

[3] Nur bei Beachtung der jeweiligen Einsatzbedingungen ist die nachweislich hohe Sicherheit, die mit dem gesetzlichen Gütezeichen zum Ausdruck gebracht wird, auch tatsächlich gegeben. Siehe auch die allgemeinen Sicherheitshinweise der Regulierungsbehörde für Telekommunikation und Post dazu (http://www.regtp.de/).

[4] Vgl. § 17 Abs. 2 Signaturgesetz vom 16.05.2001 (BGBl. I. S. 876) und § 15 Abs. 2 Signaturverordnung vom 16.11.2001 (BGBl. I. S 3074).

[5] Z.B. durch einen Warnhinweis auf dem Bildschirm.

[6] Z.B. durch Anzeigen des Dateinamens.

[7] Z.B. bei Texten/Graphiken durch **vollständige Anzeige des Inhaltes** (keine „versteckten Texte") mit eindeutiger Interpretation auf Bildschirm/Ausdruck.

[8] Als berechtigt signierende Person gilt, wer sich in der vorgesehenen Weise authentisiert hat (z.B. durch Besitz = Karte und Wissen = PIN). Es muss sichergestellt sein, dass nach Authentifizierung und der damit verbundenen „Scharfschaltung" des Signaturschlüssels nicht eine andere Person eine Signatur auslösen kann, indem mittels Hacking oder eines trojanischen Pferdes ein elektronisches Dokument (= Hashwert) „untergeschoben" wird.

[9] Dies erfordert einen gesicherten Übertragungsweg von der Eingabe der Identifikationsdaten zur Signaturerstellungseinheit.

[10] Dies kann – abhängig von der Art des Einsatzbereiches (vgl. Abschnitt 4) – z.B. auf folgende Weise erreicht werden:

- **Zugriffsicheres Verwahrgelass/zugriffsicherer (Betriebs-)Raum** für die Aufbewahrung der „Signatur-Arbeitstation", so dass ein Zugriff Unbefugter ausgeschlossen ist oder zumindest mit hoher Sicherheit erkennbar wird,
- **Prüfsoftware**, mit der sicherheitstechnische Veränderungen mit hoher Sicherheit festgestellt werden (dies erfordert, dass auch das „Prüfwerkzeug" entsprechend vor Manipulation geschützt ist) oder
- **elektronische Selbstsicherung** der Signaturanwendungskomponente, so dass diese im Falle sicherheitserheblicher Veränderungen z.B. automatisch funktionsunfähig wird und die Funktionsfähigkeit nur durch autorisiertes Wartungs-/Reparaturpersonal wieder hergestellt werden kann.

[11] In den ITSEC ist dazu folgendes ausgeführt: „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."

[12] Nach Anlage 1 Nr. 1 Signaturverordnung ist – ergänzend zu den für die Prüfstufe „EAL 3" bestehenden Prüfvorgaben – gegen ein **hohes Angriffspotential** zu prüfen und eine **vollständige Missbrauchanalyse** durchzuführen. Bei der Prüfstufe „E 2" ergibt sich diese Forderung implizit aus der Forderung nach Sicherheitsmechanismen mit der Stärke „hoch" (siehe auch Fußnote 11).

[13] Eine solche Prüfung und Bestätigung ist nur im Rahmen einer Akkreditierung vorgesehen (vgl. § 15 Abs. 7 Signaturgesetz); die geprüften und bestätigten Produkte sind am **gesetzlichen Gütezeichen** (vgl. § 15 Abs. 1 Satz 3 und Abs. 7 Signaturgesetz) zu erkennen.

[14] Gelingt es, die vorgegebene Sicherheit zu „unterlaufen", kann dies zu Folge haben, dass
- zur Signatur bestimmte Daten auf dem Weg zur Signaturerstellungseinheit unbefugt verändert,
- Daten zur Erzeugung einer elektronischen Signatur „untergeschoben" oder
- bei Prüfung von Signaturen falsche Ergebnisse angezeigt

werden.

[15] Z.B. durch Hacking oder trojanische Pferde.

[16] Im Falle eines manuellen Zugriffs Unbefugter können z.B. sichere technische Komponenten gegen manipulierte ausgetauscht werden. Bei einem Datenaustausch per Datenträger können – wie bei einem Datenaustausch über Kommunikationsnetze – z.B. trojanische Pferde eingeschleust werden.

[17] Für einen „ungeschützten Einsatzbereich" geeignete Produkte können ohne sicherheitsbedingte Einschränkung eingesetzt werden. Solche Produkte kommen wegen ihres (jedenfalls derzeit) hohen Kostenaufwandes auf absehbare Zeit jedoch nur in **Sonderfällen** (etwa bei bestimmten mobilen Einsätzen) in Betracht.

Die vorgegebene **hohe Sicherheit** (vgl. Abschnitt 2.4) muss hier mit Ausnahme der Wartung/Instandsetzung **durch Sicherheitsvorkehrungen in der Signaturanwendungskomponente selbst** erreicht werden.

Eine für einen „ungeschützten Einsatzbereich" geeignete Signaturanwendungskomponente kann z.B. durch einen „**Sicherheits-Laptop**" (mit integrierter Firewall, elektronischer Sicherung gegen unbefugte Öffnung/Veränderung, Chipkartenleser usw.) realisiert werden, der sich gegenüber dem Signaturschlüssel-Inhaber authentisiert (etwa durch Anzeige eines verschlüsselten Codewortes, das auf der Signaturerstellungseinheit – i.d.R. eine Chipkarte – gespeichert ist), woran der Signaturschlüssel-Inhaber jederzeit erkennen kann, dass es sich um sein Gerät handelt und dass dieses sich in sicherem Zustand befindet. Auf einem solchen Laptop kann zugleich auch eine sichere Verschlüsselung realisiert werden. Potentiell kommen aber u.a. auch **modifizierte PADs/Mobilfunktelefone** in Betracht.

[18] Für einen „geschützten Einsatzbereich" geeignete Produkte bilden die **Standardlösung** für Büro/Wohnung und ggf. auch im mobilen Bereich (Laptop/Handy pp.).

Die vorgegebene **hohe Sicherheit** (vgl. Abschnitt 2.4) muss hier **durch** eine **geeignete Kombination von Sicherheitsvorkehrungen in der Signaturanwendungskomponente** selbst **und** in der **Einsatzumgebung** erreicht werden.

Eine für einen „geschützten Einsatzbereich" geeignete Signaturanwendungskomponente kann z.B. durch eine „**Signatur-Software" i.V.m. einem speziellen Chipkartenleser** realisiert werden, die insbesondere einen „sicheren Kanal" zur Übertragung der
- Identifikationsdaten und
- zur Signatur bestimmten (auf dem Bildschirm angezeigten) Daten

zur Signaturerstellungseinheit bieten.

[19] Für den Einsatzbereich B. bestimmte Produkte sind nur für **Sonderfälle** geeignet, bei denen keine Anbindung an ein Kommunikationsnetz (Internet/Intranet) erforderlich ist und ein zuverlässiger Schutz vor Zutritt Unbefugter besteht (etwa in elektronischen Archiven).

Die vorgegebene **hohe Sicherheit** (vgl. Abschnitt 2.4) kann hier im wesentlichen **auf Sicherheitsvorkehrungen in der Einsatzumgebung** der Signaturanwendungskomponente **gestützt** werden.

Eine für einen „isolierten Einsatzbereich" geeignete Signaturanwendungskomponente kann allein durch „**Software**" realisiert werden. Potentielle Angriffe über manuellen Zugriff können z.B. durch eine hoch sicheren Verschluss des Betriebsraumes abgewehrt werden und potentielle Angriffe über internen Datenaustausch (Datenträger) durch den obligatorischen Einsatz geeigneter Virensuchprogramme pp..

[20] Die Übermittlung von signierten Daten erfolgt ggf. zunächst per Datenträger zu einem Rechner am Netz und von diesem online zu den gewünschten Empfängern. Bei der Überprüfung von Zertifikaten wird ggf. auf ein

speziell eingerichtetes internes Zertifikatverzeichnis (mit häufig relevanten Zertifikaten und regelmäßig aktualisierten Sperrlisten) zurückgegriffen. Auf diese Weise wird eine Anbindung an ein Kommunikationsnetz mit den damit verbundenen Risiken vermieden. Den Risiken durch die „**indirekte Anbindung“** über den Datenaustausch per Datenträger wird gesondert begegnet (siehe 2. Aufzählung).

[21] Zum Schutz vor manuellem Zugriff Unbefugter genügt es, wenn ein potentieller Zugriff Unbefugter zuverlässig erkennbar wird (etwa durch Zerstörung von Sicherungseinrichtungen) und in diesem Falle vor einer weiteren Nutzung der Signaturanwendungskomponente eine entsprechende sicherheitstechnische Überprüfung erfolgt.

[22] Eine Eignung für den Einsatzbereich B. schließt den Einsatzbereich C. und eine Eignung für den Einsatzbereich A. die Einsatzbereiche B. und C. ein.

[23] Hinweis:

- Die **nicht** schattierten Felder zeigen an, dass dort Einsatzbedingungen für die Signaturanwendungskomponente nicht zulässig sind.
- Die **hell** schattierten Felder zeigen an, dass dort Einsatzbedingungen für die Signaturanwendungskomponente nur allgemein zu benennen sind (z.B. zu keinem Zeitpunkt Netzanbindung; hoher Schutz vor manuellem Zugriff Unbefugter über isolierte Einsatzumgebung).
- Die **dunkel** schattierten Felder zeigen an, dass die Einsatzbedingungen produktspezifisch detailliert zu benennen sind.

[24] Soweit im Intranet z.B. andere Datenaustauschprotokolle verwendet werden als im Internet, sind hier auch gesonderte Maßnahmen erforderlich.

[25] Die hohe Sicherheit darf hier nicht nur über Einsatzbedingungen erreicht werden; ein wesentlicher Teil der Sicherheit muss durch konstruktiv-technische Maßnahmen in der Signaturanwendungskomponente selbst erbracht werden.

[26] IT-Plattform und die Applikationen müssen so vertrauenswürdig sein, dass die Sicherheitsfunktionen (siehe Abschnitt 2) mit hoher Sicherheit nicht beeinträchtigt werden. Sie müssen dazu insbesondere frei von Schadensprogrammen (Computerviren, trojanischen Pferde usw.) sein.

[27] Die Signaturanwendungskomponente ist seitens des Herstellers/Vertreibers entweder bereits in sicher installierter Form zur Verfügung zu stellen (Beispiel: „Sicherheits-Laptop“) oder bei einer Installation durch den Betreiber müssen sicherheitserhebliche Fehler ausgeschlossen sein, soweit es im Einflussbereich des Herstellers/Vertreibers liegt.

[28] Vor jeder Übernahme fremder Daten/Nutzung fremder Datenträger muss mit hoher Sicherheit ausgeschlossen werden, dass Schadensprogramme (z.B. Computerviren oder trojanische Pferde) eingeschleust werden.

[29] Die Eignung einer Signaturanwendungskomponente für einen „ungeschützten Einsatzbereich“ erfordert zwangsläufig eine automatische Authentifizierung des Wartungs-/Reparaturpersonals (vgl. auch Fußnote 17). Bei Signaturanwendungskomponenten, die nur für einen geschlossenen oder isolierten Einsatzbereich bestimmt sind, kann eine Authentifizierung an Hand von Ausweispapieren genügen.