Bestätigung
von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen[1] und §§ 11 Abs. 3 und 15 Signaturverordnung[2]

Bundesamt für Sicherheit in der Informationstechnik[3]
Godesberger Allee 185-189
53175 Bonn

bestätigt hiermit gemäß
§§ 15 Abs. 7 S. 1, 17 Abs. 2 SigG sowie §§ 11 Abs.3, 15 Abs. 2 und 4 SigV,
dass die

Signaturanwendungskomponente Virtuelle Poststelle des Bundes (Basis), Version 2.2.2.6

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

BSI.02070.TE.11.2007

Bundesamt für Sicherheit in der Informationstechnik

Bonn, den 27. November 2007 gez. Helmbrecht

Dr. Helmbrecht
Präsident

Das Bundesamt für Sicherheit in der Informationstechnik ist, auf Grundlage des BSI-Errichtungsgesetzes vom 17.12.1990, Bundesgesetzblatt I S. 2834 und gemäß der Veröffentlichung im Bundesanzeiger Nr. 31 vom 14. Februar 1998, Seite 1787, zur Erteilung von Bestätigungen für Produkte gemäß § 15 Abs. 7 S. 1 (oder § 17 Abs. 4) SigG ermächtigt.

---

1 Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22) geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04.01.2005 (BGBl. I S. 2)

2 Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59) geändert durch 1. SigÄndG

3 Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn, Postfach 200363, 53133 Bonn, Tel: +49(0)3018 9582-0, Fax: +49(0)3018 9582-5477, E-Mail: bsi@bsi.bund.de, Web: www.bsi.bund.de

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Signaturanwendungskomponente, Virtuelle Poststelle des Bundes, Version 2.2.2.6 (Basis)[4].

1.1 Auslieferung und Lieferumfang:

Das Produkt wird auf CD-ROM und online als Archiv an den Betreiber ausgeliefert. Separat von der Auslieferung veröffentlicht der Hersteller einen SHA-1 Wert über die ausgelieferte Software auf einer gesicherten Webseite. Dieser Hashwert ist auch nach Tabelle 1 aufgeführt. Bei beiden Auslieferungswegen wird der Empfänger darauf hingewiesen, dass er mit einem geeigneten Werkzeug[5] den Hashwert über die erhaltene Software bilden und mit dem veröffentlichten Wert vergleichen muss.

1.2 Antragsteller dieser Bestätigung:

Bundesministerium des Innern
Alt-Moabit 101D
10559 Berlin

1.3 Hersteller und Vertreiber des Produkts:

bremen online services
Entwicklungs- und Betriebsgesellschaft mbH & Co. KG
Am Fallturm 9
28359 Bremen
info@bos-bremen.de
www.bos-bremen.de

1.4 Lieferumfang des Produktes:

Die Tabelle 1 beschreibt den Lieferumfang der Basiskomponente:

Nr.	Art	Teil	Version	Datum	Art der Auslieferung
1	Software	VPS Basiskomponente	2.2.2.6	06.09.2007	auf CD-ROM oder als Download
2	Dokument	Betriebshandbuch	2.2.5	06.09.2007	pdf-Datei auf CD-ROM oder als Download
3	Dokument	Schnittstellenbeschreibung des Kernsystems	2.3.2	06.09.2007	pdf-Datei auf CD-ROM oder als Download

Tabelle 1: Lieferumfang der Basiskomponente

[4] Im Weiteren Basiskomponente genannt.
[5] Der Hersteller nennt als Beispiel das Tool `sha1sum`, das unter der GPL im Sourcecode und als Binary für alle unterstützten Betriebssysteme erhältlich ist.

Der SHA1-Hashwert der ausgelieferten Datei ist:

dc 13 25 ba 2b f0 97 87 d2 72 9f 32 2b 64 e6 d4 25 a5 e6 22

2 Funktionsbeschreibung

2.1 Kurzbeschreibung

Im Rahmen des Projektes BundOnline 2005 wurde die Virtuelle Poststelle des Bundes entwickelt. Sie stellt als zentrales Kommunikations-Gateway Sicherheitsdienste für die gesicherte Kommunikation zwischen Behörden und externen Kommunikationspartnern (Bürger, Wirtschaft und andere Behörden) bereit. Dieses komplexe Produkt wird in drei Verfahren mit den Evaluationsgegenständen Basiskomponente (EVG 1, blau markiert in Abbildung 1 und Gegenstand dieser Bestätigung), OSCI[6]-Komponente (EVG 2, gelb markiert in Abbildung 1) und Verifikationsmodul (EVG 3, orange markiert in Abbildung 1) evaluiert, zertifiziert und bestätigt. Ausschließlich die in Abbildung 1 farblich gekennzeichneten Teile der Virtuellen Poststelle des Bundes werden für die Erstellung der qualifizierten elektronischen Signatur benötigt und sind daher Bestandteil von Evaluierungs- und Bestätigungsverfahren. Alle weiteren Anteile, die in Abbildung 1 nicht farblich markiert sind, sind demzufolge nicht Gegenstand einer Evaluierung und Bestätigung.

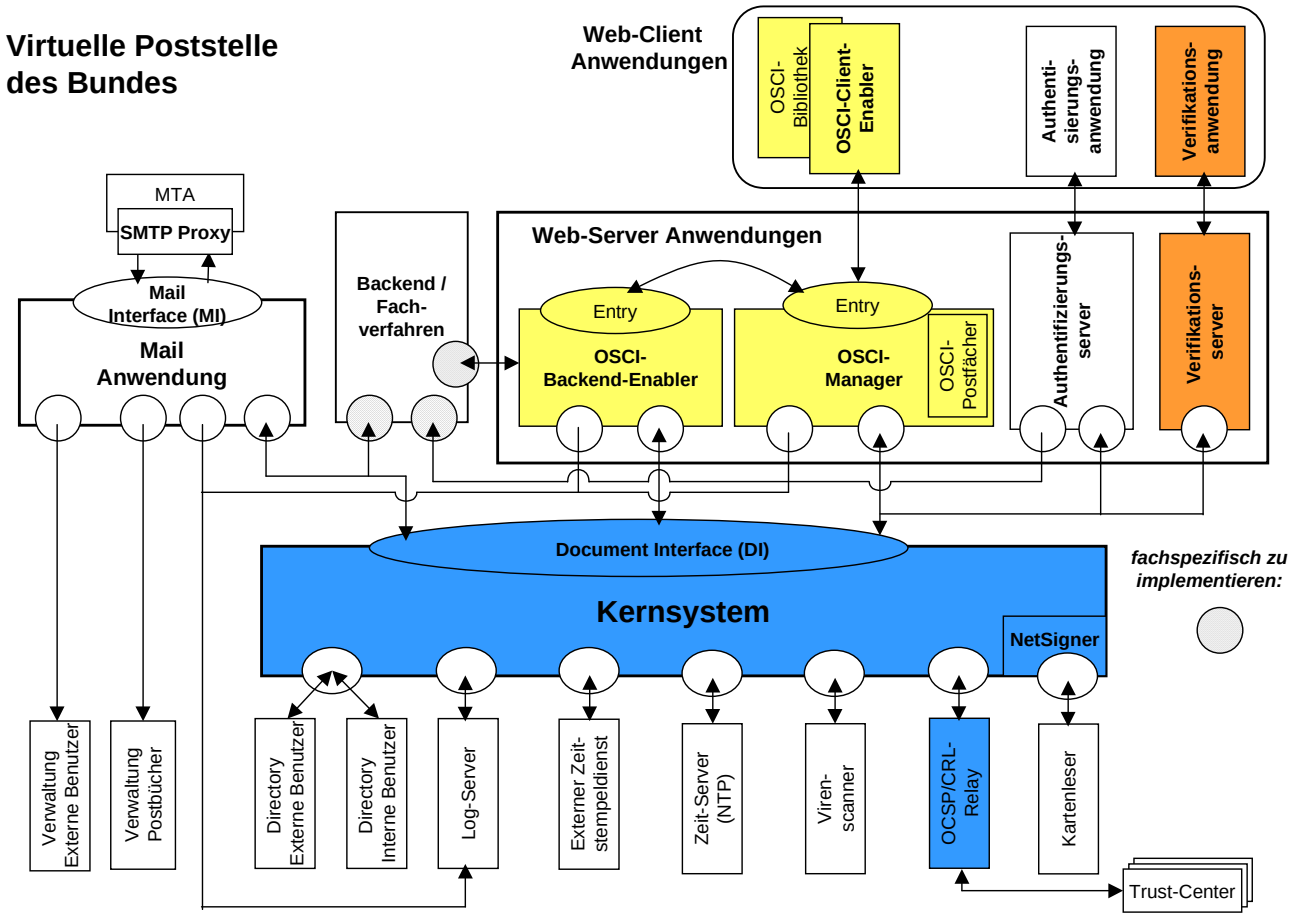

Abbildung 1: Aufbau der Virtuellen Poststelle des Bundes

Die Evaluierung der OSCI-Komponente (EVG 2) beinhaltet eine Funktionsbibliothek (OSCI-Bibliothek, OSCI-Client-Enabler) für die sichere Anzeige und das Signieren von Dokumenten am Arbeitsplatz sowie zur Kommunikation über das OSCI-Protokoll. Die

[6] Online Services Computer Interface, www.osci.org

weiteren Anteile der OSCI-Komponente bilden eine Funktionsbibliothek zur Integration in ein Fachverfahren (OSCI-Backend-Enabler), die eine Anbindung über das OSCI-Protokoll erlaubt, sowie die zentrale Serverkomponente für den Betrieb einer OSCI-konformen IT-Infrastruktur (OSCI-Manager).

Das Verifikationsmodul (EVG 3) umfasst eine Signaturanwendungskomponente für das Verifizieren von Signaturen und Zertifikaten am Arbeitsplatz des Endnutzers. Diese besteht aus einer Serverkomponente (Verifikationsserver) und einem dazugehörigen Client (Verifikationsanwendung).

Bestandteil dieser Bestätigung ist ausschließlich die Basiskomponente (EVG 1), die in Abbildung 1 aus den Teilen Kernsystem mit NetSigner und OCSP/CRL-Relay besteht. Da sowohl die OSCI-Komponente als auch das Verifikationsmodul dem Endnutzer Möglichkeiten zum Zugriff auf Funktionalitäten der Basiskomponente bereitstellen, ist die Evaluierung und Bestätigung der Basiskomponente Grundlage für eine Nutzung der Virtuellen Poststelle des Bundes im Rahmen der qualifizierten elektronischen Signatur. Die Basiskomponente stellt als zentrale Komponenten folgende Funktionalitäten zur Verfügung:

- Unterstützung bei der Erzeugung qualifizierter elektronischer Batchsignaturen[7];
- mathematische Prüfung qualifizierter elektronischer Signaturen (Verifikation);
- Statusprüfung qualifizierter Zertifikate (Validierung).

Systeme, welche Funktionalitäten der Basiskomponente nutzen wollen, werden als autorisiert anfordernde Systeme[8] bezeichnet.

Die Basiskomponente stellt selbst nur einen Teil der Funktionalität zur Verfügung, die vom Signaturgesetz bzw. der Signaturverordnung gefordert wird. So obliegt z.B. die Funktionalität, dass „die Erzeugung einer Signatur vorher eindeutig angezeigt wird“ (§ 15 Abs. 2 SigV), dem anfordernden System in der IT-Umgebung, welches einen Auftrag an die Basiskomponente absendet. Die Basiskomponente erlaubt lediglich einem Inhaber eines Signaturschlüssels, bestimmte Vorgaben zu machen. Dazu gehört die maximale Zeit oder Anzahl für die Erstellung von Signaturen sowie die Festlegung der autorisiert anfordernden Systeme, die auf die Karte des Signaturschlüssel-Inhabers zugreifen dürfen. Ähnliches gilt auch für die Anteile von § 17 Abs. 2 SigG. Der Bezug von Daten zur Signatur („...auf welche Daten sich die Signatur bezieht...“) und das Anzeigen signierter Daten („...nach Bedarf auch den Inhalt der zu signierenden Daten hinreichend erkennen lassen...“) muss ebenfalls durch das anfordernde System in der IT-Umgebung der Basiskomponente gewährleistet werden. Die autorisiert anfordernden Systeme müssen auch sicherstellen, dass einer Batchsignatur ausschließlich praktisch gleiche Vorgänge zugeführt werden, da die Basiskomponente keine Analyse der Inhalte vornimmt. Daher müssen anfordernde Systeme bestätigt werden, bevor sie zusammen mit der Basiskomponente zur Erstellung von qualifizierten elektronischen Signaturen genutzt werden können. Die anfordernden Systeme sind nicht Bestandteil dieser Bestätigung.

Die Kommunikation mit den anfordernden Systemen sichert die Basiskomponente durch den Einsatz von elektronischen Signaturen ab. Anforderungen zum Erzeugen

[7] Eine Batchsignatur ist eine serverbasiert erzeugte SigG-konforme qualifizierte elektronische Signatur, bei der eine große Anzahl praktisch gleicher Vorgänge – z. B. Rechnungen, die sich ‚nur’ im Betrag und der Zustelladresse unterscheiden – in einer besonders gesicherten Umgebung automatisiert abgearbeitet werden.

[8] Ein anforderndes System ist ein System in der IT-Umgebung der Basiskomponente, das eine Fachaufgabe wahrnimmt und die Funktionen der Basiskomponente im Zusammenhang mit qualifizierten elektronischen Signaturen nutzt. Ein anforderndes System ist immer eine Signaturanwendungskomponente und erfüllt daher bestimmte Vorgaben von Signaturgesetz und –verordnung (s. Tabelle 3)

qualifizierter elektronischer Batchsignaturen werden durch eine elektronische Signatur gegen eine Integritätsverletzung geschützt, die ein autorisiert anforderndes System erstellt. Umgekehrt versieht die Basiskomponente Ergebnisse von Prüfungen qualifizierter Zertifikate oder qualifizierter elektronischer Signaturen mit einer elektronischen Signatur, so dass ein anforderndes System die Integrität der Ergebnisse überprüfen kann. Die so erreichte Absicherung der Kommunikation ist Bestandteil dieser Bestätigung.

Für die Anforderung von qualifizierten elektronischen Batchsignaturen wird auf jedem autorisiert anfordernden System ein eigenes Serverzertifikat mit dem geheimen Signaturschlüssel hinterlegt, wobei der Schutz des geheimen Signaturschlüssels dem anfordernden System oder seiner Umgebung obliegt. Das Serverzertifikat mit dem dazugehörigen öffentlichen Schlüssel ist der Basiskomponente zugänglich und zur vereinfachten Verwaltung einer sog. Rolle zugeordnet. Durch Anzeige einer solchen Rolle kann z.B. dem Signaturschlüssel-Inhaber das zugeordnete Serverzertifikat und damit das anfordernde System, das auf seine Signaturkarte zugreifen kann, übersichtlich angezeigt werden.

Für die Signatur der Ergebnisse von Prüfungen qualifizierter Zertifikate oder qualifizierter elektronischer Signaturen verfügt die Basiskomponente über ein Serverzertifikat mit geheimem Signaturschlüssel, der aufgrund der Anforderungen an den Betrieb durch eine gesicherte Umgebung geschützt wird. Das Serverzertifikat mit dem öffentlichen Schlüssel zur Prüfung der Signatur der Basiskomponente wird auf all den Systemen verteilt, die eine solche Antwort anfordern dürfen. Die Serverzertifikate sind nicht öffentlich zugänglich und nicht auf eine Person ausgestellt, so dass mit ihnen nur elektronische Signaturen erstellt werden können.

Da Serverzertifikate nicht öffentlich abprüfbar sind, verfügen sie über keine zeitliche Begrenzung und werden nicht gesperrt. Liegt der Verdacht der Kompromittierung vor, so müssen sie ausgetauscht werden. Für die Beschaffung, sichere Verteilung und ggf. den Austausch der Serverzertifikate von Basiskomponente oder anforderndem System mit den öffentlichen und geheimen Schlüsseln sind die Schlüsseladministratoren (s.u.) zuständig. Die eingesetzten Algorithmen zur Signatur von Daten mit Hilfe der Serverzertifikate sind durch die Bundesnetzagentur als geeignet für die Verwendung bei der qualifizierten elektronischen Signatur eingestuft.

Die mathematische Prüfung qualifizierter elektronischer Signaturen sowie die Statusprüfung qualifizierter Zertifikate wird, abgesehen von der authentischen Darstellung des Ergebnisses für den Benutzer, durch die Basiskomponente vollständig bearbeitet.

Technisch gesehen besteht die Basiskomponente aus den Teilsystemen

- Kernsystem mit NetSigner und
- OCSP/CRL-Relay,

inklusive einer Administrationsanwendung als Graphical User Interface (GUI) zur Bedienung. Abbildung 2 illustriert die Teilsysteme der Basiskomponente (gelb markiert), für welche die vorliegende Bestätigung gilt.

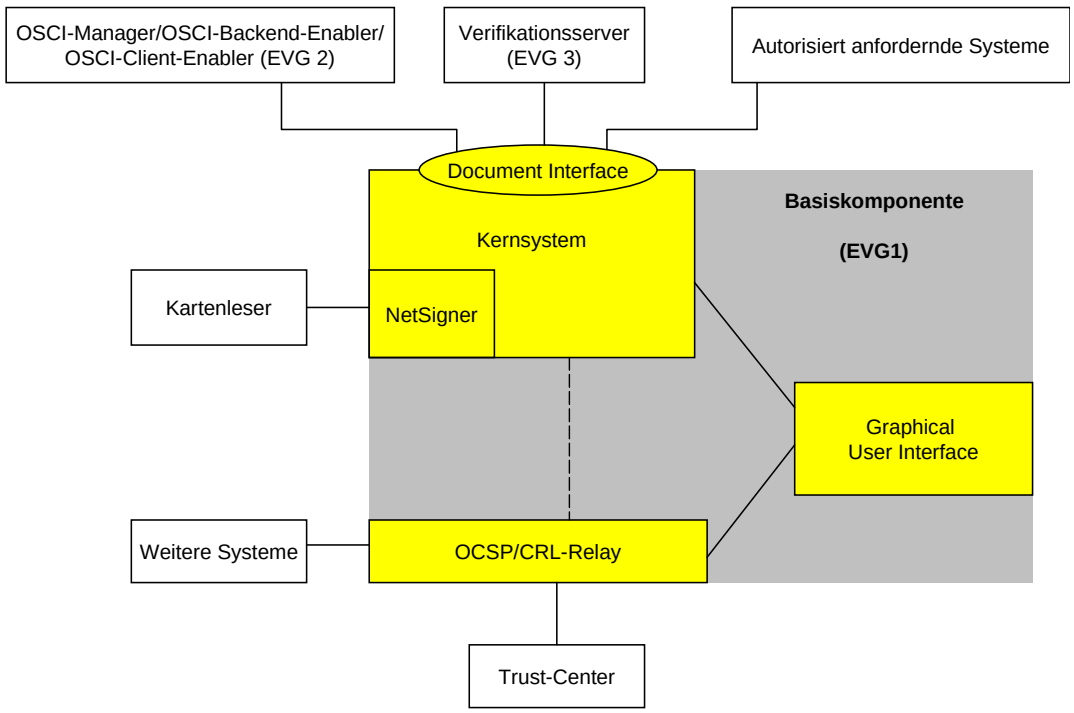

Abbildung 2: Technischer Aufbau der Basiskomponente

Kernsystem (mit NetSigner) und OCSP/CRL-Relay können voneinander getrennt betrieben werden. Dies bedeutet, dass die Verbindung nicht innerhalb eines LANs (Local Area Network), sondern über ein Weitverkehrsnetz (Wide Area Network – WAN) hergestellt werden kann.

Die wesentlichen Aufgaben der Teilsysteme sind:

- Das Kernsystem nimmt Anforderungen von außen über eine Schnittstelle (sog. Document Interface) an.
- Der NetSigner ist dafür zuständig, zu signierende Daten der sicheren Signaturerstellungseinheit über einen angeschlossenen Kartenleser zuzuführen. Hierbei können mehrere Kartenleser angeschlossen werden, die Karten unterschiedlicher Signaturschlüssel-Inhaber enthalten können.
- Das OCSP/CRL-Relay stellt die Gültigkeit eines Zertifikats fest und nutzt dazu verschiedene Verzeichnisdienste.
- Auf ein OCSP/CRL-Relay können neben dem Kernsystem andere Systeme über eine zweite Schnittstelle, die ein anderes Protokoll unterstützt, zugreifen. Diese Systeme sind nicht Bestandteil der Bestätigung.

Zum Schutz vor Veränderungen wird die Basiskomponente auf Servern in einem „geschützten Einsatzbereich (Regelfall/Standardlösung)“[9] betrieben, und zwar in einem „zugriffsicheren Verwahrgelass/zugriffsicherer (Betriebs-)Raum für die Aufbewahrung der „Signatur-Arbeitstation“, so dass ein Zugriff Unbefugter ausgeschlossen ist oder zumindest mit hoher Sicherheit erkennbar wird“[9]. Nachdem eine Signaturkarte für die Erzeugung von Batchsignaturen vom Signaturschlüssel-Inhaber freigeschaltet wurde, arbeitet die Basiskomponente im Produktivbetrieb automatisiert und ohne menschliche Interaktionen.

[9] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur), „Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten– Arbeitsgrundlage für Entwickler/ Hersteller und Prüf-/Bestätigungsstellen“, Version 1.4, 19.07.2005.

Hinsichtlich des Schutzes vor sicherheitstechnischer Veränderung gelten für autorisiert anfordernde Systeme die gleichen Bedingungen wie für die Basiskomponente. Es muss sichergestellt sein, dass die auf den anfordernden Systemen vorhandenen geheimen Signaturschlüssel nicht kompromittiert werden können, damit die Sicherheitsmaßnahmen wirken.

2.2 Funktionsbeschreibung des Produkts

Insgesamt beinhaltet das Produkt drei Sicherheitsfunktionen, die im Folgenden beschrieben sind.

Sicherheitsfunktion SF1: „Unterstützung bei der Erzeugung qualifizierter elektronischer (Batch-)Signaturen (Zuführen zu signierender Dokumente zu einer sicheren Signaturerstellungseinheit)“

Die Sicherheitsfunktion SF1 umfasst sowohl den Anstoß zur Erzeugung von Batchsignaturen als auch die Konfiguration der Basiskomponente.

Anstoß zur Erzeugung von Batchsignaturen

Das Kernsystem erhält von einem anfordernden System über eine Schnittstelle die Anforderung, Daten serverbasiert mit einer Batchsignatur zu versehen. Die Daten bestehen aus den Hashwerten der Dokumente, die qualifiziert elektronisch signiert werden sollen. Die Hashwertbildung findet auf dem autorisiert anfordernden System statt. Die Anforderung enthält insbesondere

- die zu signierenden Daten (Hashwert des Dokuments),
- die auszuführende Aktion (OperationId)
- sowie eine Kennung über das anfordernde System (SystemId).

Die übergebenen Hashwerte sind elektronisch signiert. D.h., dass jedes anfordernde System über einen privaten Schlüssel und ein entsprechendes Serverzertifikat (X.509-konform) verfügt, das von der Basiskomponente zur Prüfung der elektronischen Signatur verwendet wird. Als Signatur-Algorithmen für die Serverzertifikate wird SHA-1 zusammen mit RSA (Schlüssellänge von 2048 Bit) eingesetzt. Die Serverzertifikate mit den zugehörigen öffentlichen Schlüsseln sind in der Basiskomponente hinterlegt.

Durch die elektronische Signatur der Hashwerte wird die Autorisierung der Signaturanfrage zur Erzeugung einer Batchsignatur sichergestellt und gewährleistet, dass nur die Daten signiert werden, die das anfordernde System dem Signierprozess zuführen möchte. Da die zu signierenden Dokumente nicht an die Basiskomponente übergeben werden, kann die Gleichartigkeit[10] der Dokumente in der Anforderung nicht geprüft werden. Dies muss durch das anfordernde System sichergestellt werden und wird als Anforderung an die Einsatzumgebung gefordert (siehe Kapitel 3.2). Daher ist die Sicherstellung der Gleichartigkeit der qualifiziert elektronisch signierten Daten nicht Bestandteil dieser Bestätigung.

Im Kontext der Signaturerstellung wird die Basiskomponente intern wie folgt genutzt:

- Das Kernsystem prüft, ob das anfordernde System die Batchsignatur-Funktion nutzen darf. Dafür sind im Kernsystem bestimmte Regeln konfiguriert, die Zugriffsmöglichkeiten in Abhängigkeit von SystemId und OperationId definieren.

[10] Siehe die Darstellung der Bundesnetzagentur zur FAQ 18 unter www.bundesnetzagentur.de (http://www.bundesnetzagentur.de/enid/Elektronische_Signatur/FAQ_pm.html).

Bei einer Anfrage vergleicht das Kernsystem die SystemId und die OperationId mit den im Regelwerk enthaltenen Regeln und erlaubt bzw. verweigert den Zugriff.

- Zum Signieren werden die zu signierenden Hashwerte vom Kernsystem dem NetSigner zugeführt, an dem die Chipkartenleser mit den Signaturkarten angeschlossen sind. Anschließend empfängt das Kernsystem die Signatur bzw. im Fehlerfall eine Fehlermeldung vom NetSigner. Das Kernsystem liefert im Anschluss die signierten Daten resp. die Fehlermeldung an das anfordernde System zurück.
- Der NetSigner führt zu signierende Hashwerte der sicheren Signaturerstellungseinheit zu. Dabei führt der NetSigner folgende Prüfung durch:
  - Es wird geprüft, dass die Signatur der Anforderung mathematisch korrekt ist. Der für die Verifikation der Anfrage benötigte öffentliche Schlüssel des anfordernden Systems liegt in Form eines Serverzertifikats in der Basiskomponente – im Sinne eines Trust Anchors – vor. Eine separate Übertragung des Zertifikats bei jeder Anforderung von Batchsignaturen findet nicht statt.
  - Zudem wird geprüft, dass die Zuordnung vom Serverzertifikat der Signier-Anforderung des anfordernden Systems zur angeschlossenen Signaturkarte für die Erzeugung der Batchsignatur korrekt ist. Dies bedeutet, dass ein anforderndes System (gekennzeichnet durch Serverzertifikat und Rolle) die sichere Signaturerstellungseinheit, die die Batchsignatur erzeugen soll, nutzen darf.
  - Es wird geprüft, ob das Zeitfenster für die Erzeugung von Batchsignaturen gültig bzw. die gültige Anzahl von Batchsignaturen noch nicht erreicht ist.

Die Prüfung der elektronischen Signatur der Anforderung schlägt immer fehl, wenn das über die SystemId zugeordnete Serverzertifikat nicht vorhanden ist. Wie in Kapitel 2.1 erläutert, werden kompromittierte Zertifikate ausgetauscht, anstelle sie zu sperren.

Sind alle Prüfungen positiv verlaufen, werden die zu signierenden Hashwerte der sicheren Signaturerstellungseinheit (Signaturkarte) zugeführt. Anschließend werden die signierten Daten bzw. eine Fehlermeldung an das autorisiert anfordernde System zurückgeliefert.

Bevor Batchsignaturen erzeugt werden können, muss der Signaturschlüssel-Inhaber initial seine sichere Signaturerstellungseinheit per PIN-Eingabe freischalten. Dazu wird ihm angezeigt,

- welches System bzw. welche Rolle zu welchem Zweck (Fachaufgabe)
- innerhalb welchen Zeitfensters bzw. für welche Anzahl von Batchsignaturen

seine sichere Signaturerstellungseinheit nutzen kann. Die Bedienung des anfordernden Systems und damit das Auslösen einer Signaturanforderung erfolgt durch berechtigt signierende Personen, die sich an dem anfordernden System erfolgreich identifiziert und authentisiert haben. Wird eine Signaturkarte aus dem Chipkartenleser entfernt, erhält der Signaturschlüssel-Inhaber eine entsprechende Mitteilung per E-Mail. Diese Signalisierung ist Teil der Sicherheitsfunktion SF1 und damit Gegenstand von Evaluierung und Bestätigung.

Konfiguration der Basiskomponente

Die Aufgaben, die für den ordnungsgemäßen Betrieb zu erledigen sind, sind in Tabelle 2 zusammenfassend aufgeführt und verschiedenen Benutzerrollen zugeteilt.

Genauere Beschreibungen für die einzelnen Tätigkeiten der Benutzerrollen finden sich in den Betriebshandbüchern zum Kernsystem, OCSP/CRL-Relay und zur Administrationsanwendung (siehe Tabelle 1). Eine umfangreiche graphische Benutzeroberfläche erlaubt die Erledigung dieser Aufgaben. Die Evaluierung umfasst insbesondere die Prüfung, dass die Trennung der Benutzerrollen entsprechend der Konfiguration durchgesetzt wird, eingestellte Konfigurationen wirksam sind und ein Benutzer sich bei der Basiskomponente entsprechend seiner Benutzerrolle identifizieren und autorisieren muss.

Benutzerrolle	**Aufgaben**
Security-Administrator	Die Basiskomponente erlaubt dem Security-Administrator • die Konfiguration der Authentisierungssysteme (z.B. Rollen und Regeln im Regelwerk setzen, ändern und löschen), • die Verwaltung der unterschiedlichen Methoden, welche die Basiskomponenten zur Verfügung stellen (kryptographische Funktionen, Sicherheitsdienst, Anbindung externer Systeme), • das Starten, Stoppen und Rücksetzen der Basiskomponente, • Einbringung von Patches, Austausch von Software-Komponenten, • Datensicherung. Zugriffe auf kryptographische Schlüssel oder Signaturerstellungseinheiten sind dem Security-Administrator nicht erlaubt.
Schlüssel-Administrator	Dem Schlüssel-Administrator werden die folgenden Tätigkeiten erlaubt: • Die Verwaltung (Beschaffung, Verteilung, Installation und Austausch) der in der Basiskomponente und den anfordernden Systemen benötigten kryptographischen Schlüssel und Sicherheitsanker. • Die Einstellung von Standardwerten zur Begrenzung für die Erzeugung von Batchsignaturen entweder hinsichtlich der Anzahl zu erzeugender Batchsignaturen oder des Zeitfensters, in dem Batchsignaturen erzeugt werden können. Bei der Freischaltung einer Signaturkarte werden diese Werte dem Signaturschlüssel-Inhaber angezeigt und können von diesem geändert werden. • Die Zuordnung von Signaturkarten zu anfordernden Systemen. Zugriffe des Schlüssel-Administrators auf weitere Systemparameter wie z.B. Rechte oder Rollen werden durch die Basiskomponente verhindert.
Signaturschlüssel-Inhaber	Die Basiskomponente sichert zu, dass der Signaturschlüssel-Inhaber ausschließlich über die ihm zugeordnete sichere Signaturerstellungseinheit verfügen kann. Daher sind ihm die folgenden Tätigkeiten erlaubt: • Freischaltung der sicheren Signaturerstellungseinheit nach

Benutzerrolle	Aufgaben
	Aufforderung durch die Basiskomponente. • Änderung der Voreinstellungen für die Erzeugung von Batchsignaturen (Zeitfenster oder Anzahl) im Beisein eines Schlüssel-Administrators.
Revisor	Hauptaufgabe des Revisors ist die Prüfung der ordnungsgemäßen Konfiguration gemäß den Hinweisen aus den Administrationshandbüchern und den spezifischen Anforderungen des Betreibers. Dazu überprüft er die Sicherheitsparameter (nur lesender Zugriff) und veranlasst ggf. eine Änderung durch den zuständigen Administrator. Er hat keine Möglichkeit, Werte an der Basiskomponente selbst zu ändern.

Tabelle 2: Benutzerrollen und ihre Tätigkeiten innerhalb der Basiskomponente

Abgesehen von den Personen, die den Benutzerrollen aus Tabelle 2 zugeordnet sind, ist für den Betrieb der zu Grunde liegenden IT auch ein System-Administrator erforderlich.

Im Rahmen des Betriebs sind den Benutzerrollen weitere Tätigkeiten zugeordnet, die aber nicht über evaluierte und bestätigte Funktionalitäten der Basiskomponente bearbeitet werden und die daher in der Tabelle 2 nicht aufgeführt sind.

Der Hersteller verlangt vom Betreiber, organisatorisch ein Vier-Augen-Prinzip bei den folgenden Tätigkeiten einzurichten:

- Der Security-Administrator wird von einem Revisor bei der Konfiguration der Authentisierungssysteme für die Anbindung der externen Systeme beaufsichtigt.
- Ein Signaturschlüssel-Inhaber erhält den Zugang zum Betriebsraum nur durch einen Schlüssel-Administrator, der den Aufenthalt überwacht. Somit kann der Signaturschlüssel-Inhaber nicht ungesehen auf andere als seine eigene Signaturkarte zugreifen und sich bei der Einstellung von Begrenzungen für Batchsignaturen beraten lassen.

Zusammenfassung der Funktionalität der Sicherheitsfunktion SF1

Zusammenfassend ist in der Sicherheitsfunktion SF1 die folgende Funktionalität enthalten:

- Bei der Freischaltung einer sicheren Signaturerstellungs-Einheit wird dem Signaturschlüssel-Inhaber angezeigt, von welcher Fachanwendung mit welchen Begrenzungen (Anzahl an Signaturen oder Zeitbegrenzung) seine Karte genutzt wird, wobei er die Begrenzungen verändern kann.
- Bei der Anforderung von Batchsignaturen erfolgt eine mathematische Prüfung der elektronischen Signatur zur Prüfung der Integrität.
- Die Zulässigkeit der Anforderung von Batchsignaturen eines anfordernden Systems wird gegen die im Regelwerk abgelegten Regeln geprüft. Dies umfasst auch einen Abgleich der Berechtigung des anfordernden Systems zum Zugriff auf die angegebene Signaturerstellungseinheit.
- Signaturen werden nur erstellt, falls eine der angegebenen Beschränkungen (Zeitfenster oder Anzahl von qualifizierten elektronischen Signaturen) nicht überschritten worden ist.

- Zu signierende Hashwerte werden an die entsprechende sichere Signaturerstellungseinheit weitergeleitet. Die erstellten Signaturen werden durch die Basiskomponente mathematisch geprüft.
- Der konfigurierte Signaturschlüssel-Inhaber wird per E-Mail benachrichtigt, wenn die sichere Signaturerstellungseinheit aus dem angeschlossenen Kartenleser entfernt wurde.
- Durchsetzen einer Trennung von Verantwortlichkeiten durch die Beschränkung von Aufgaben auf unterschiedliche Benutzerrollen. Die Administrationsanwendung, mit der die Basiskomponente konfiguriert werden kann, ist Teil der Evaluierung und Bestätigung.

Sicherheitsfunktion SF2 „Mathematische Prüfung qualifizierter Signaturen (Verifizieren)“

Das Kernsystem erhält von einem System die Anforderung, die mathematische Korrektheit einer qualifizierten elektronischen Signatur zu prüfen. Dazu prüft das Kernsystem die Signatur mittels zugehörigem Prüfschlüssel (öffentlicher Schlüssel des qualifizierten Zertifikats) und geeigneten kryptographischen Verfahren, stellt das Ergebnis (korrekte oder nicht korrekte Signatur oder Fehlermeldung) fest und versieht das Ergebnis der Verifikation mit einer elektronischen Signatur. Das der Signatur zugrunde liegende Serverzertifikat liegt in der Basiskomponente vor. Anschließend wird das Ergebnis der Verifikation an das anfordernde System zurückgeliefert.

Ein anforderndes System muss sich gegenüber der Basiskomponente durch Angabe einer bestimmten Kennung (SystemId) identifizieren und die gewünschte Operation angeben (OperationId). Die Basiskomponente prüft vor der Durchführung der mathematischen Prüfung, ob die Kombination von SystemId und OperationId gemäß der im Regelwerk eingestellten Regeln erlaubt ist.

Sicherheitsfunktion SF3 „Statusprüfung qualifizierter Zertifikate (Validieren)“

Die Basiskomponente erhält von einem System der IT-Umgebung die Anforderung, die Gültigkeit eines Zertifikats festzustellen, wobei Gültigkeit gemäß SigG die Prüfung impliziert, ob ein nachgeprüftes qualifiziertes Zertifikat im jeweiligen Zertifikatsverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt war. Eine Anforderung wird innerhalb der Basiskomponente durch das Kernsystem und das OCSP/CRL-Relay folgendermaßen bearbeitet:

1. Das Kernsystem erhält diese Anforderung und prüft, ob das anfordernde System zu dieser Operation berechtigt ist. Fällt die Prüfung positiv aus, wird die Anforderung an das OCSP/CRL-Relay weitergeleitet (siehe Schritt 2). Das mit einer elektronischen Signatur versehene Ergebnis der Validierung des OCSP/CRL-Relays umfasst eine Interpretation der Validierung (gültig und nicht gesperrt, unbekannt oder gesperrt) und die Verzeichnisdienst-Auskünfte. Das Kernsystem liefert dieses elektronisch signierte Ergebnis der Validierung an das anfordernde System zurück.
2. Das OCSP/CRL-Relay erhält – entweder vom Kernsystem oder einem anderen System – die Anforderung, die Gültigkeit eines Zertifikats festzustellen. Dazu validiert das OCSP/CRL-Relay das entsprechende Zertifikat entlang der Zertifikatskette. Das OCSP/CRL-Relay stellt für das angeforderte qualifizierte Zertifikat fest, ob das qualifizierte Zertifikat zum angegebenen Zeitpunkt bzw. zum Prüfzeitpunkt (wenn kein Zeitpunkt explizit übergeben wurde) vorhanden und nicht gesperrt war und der Gültigkeitszeitraum des qualifizierten Zertifikats zum

angegebenen Zeitpunkt bzw. Prüfzeitpunkt (wenn kein Zeitpunkt explizit übergeben wurde) bereits begonnen hatte und noch nicht abgelaufen war. Darüber hinaus stellt das OCSP/CRL-Relay für Ausstellerzertifikate fest,

- ob ein Ausstellerzertifikat (in der Zertifikatskette) zum Signierzeitpunkt des ausgestellten Zertifikats vorhanden und
- nicht gesperrt war und
- der Gültigkeitszeitraum eines Ausstellerzertifikats (in der Zertifikatskette) zum Signierzeitpunkt des ausgestellten Zertifikats bereits begonnen hatte und noch nicht abgelaufen war.

In diesem Zusammenhang fordert das OCSP/CRL-Relay Zertifikatsstatus-Anfragen via Online Certificate Status Protocol (OCSP) und Sperrlisten via Certificate Revocation Lists (CRLs) sowie benötigte Zertifikate via Lightweight Directory Access Protocol (LDAP) an. Das OCSP/CRL-Relay prüft in diesem Kontext die mathematische Korrektheit qualifizierter elektronischer Signaturen (Zertifikate, Antworten auf OCSP-Anfragen und CRLs) und verwendet das Ergebnis (gültige oder ungültige Signatur oder Fehlermeldung) weiter. Das Ergebnis der Validierung umfasst eine Interpretation der Validierung (gültig und nicht gesperrt, unbekannt oder gesperrt) und die Verzeichnisdienst-Auskünfte; diese beinhalten die Ergebnisse der OCSP-Anfrage bzw. optional Sperrlisten. Für Zertifikatsprüfungen via LDAP werden nur die Interpretationen zurückgeliefert. Das Ergebnis der Validierung signiert das OCSP/CRL-Relay mit einer elektronischen Signatur. Der Signaturschlüssel für diese Signatur liegt dafür im OCSP/CRL-Relay vor. Anschließend liefert das OCSP/CRL-Relay dieses elektronisch signierte Ergebnis der Validierung an das System zurück, das die Anfrage gestellt hat. Der öffentliche Schlüssel, der zu dem geheimen Signaturschlüssel passt, muss auf dem anfordernden System in Form eines Trust-Anchors vorhanden sein. Wie in Tabelle 2 und Kapitel 2.1 beschrieben ist der Schlüssel-Administrator dafür zuständig, die entsprechenden Zertifikate auf die anfordernden Systeme zu verteilen.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Das Produkt erfüllt die nachfolgend aufgeführten Anforderungen teilweise. Die Einschränkungen sind jeweils im Anschluss an die Anforderung angegeben.

SigV

- § 15, Absatz 2, Nr. 1b), „eine Signatur nur durch die berechtigt signierende Person erfolgt“, wobei ein anforderndes System die Autorisierung zum Anstoßen der Erzeugung von Batchsignaturen übernimmt und die Gleichartigkeit der Dokumente sicherstellt. Die berechtigt signierende Person muss sich an dem anfordernden System erfolgreich identifizieren und authentifizieren, um Batchsignaturen anstoßen zu können. Ein anforderndes System ist nicht Bestandteil dieser Bestätigung.
- § 15, Absatz 2, Nr. 2a), „die Korrektheit der Signatur zuverlässig geprüft“. Die authentische Anzeige des Ergebnisses obliegt dem System, das die Verfikation der Signatur angefordert hat und ist somit nicht Bestandteil der Bestätigung.
- § 15, Absatz 2, Nr. 2b), „nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikats-Verzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren“. Die authentische Anzeige des Ergebnisses obliegt dem System, das die Validierung des qualifizierten Zertifikats angefordert hat, und ist somit nicht Bestandteil der Bestätigung.
- § 15, Absatz 4, „Sicherheitstechnische Veränderungen an technischen Komponenten [...] müssen für den Nutzer erkennbar sein“. Das Produkt leistet an dieser Stelle nur die Benachrichtigung des Nutzers, wenn seine sichere Signaturerstellungseinheit nicht mehr vorhanden ist. Eine Anzeige von Änderungen an der Software des Produktes ist nicht Bestandteil dieser Bestätigung, sondern muss durch die Einsatzbedingungen[9] sichergestellt werden (siehe auch Tabelle 3, Annahme A.Betrieb).

3.2 Einsatzbedingungen

Die Bestätigung gilt unter der Voraussetzung, dass folgende Annahmen an die Einsatzbedingungen gewährleistet sind:

Annahme	Beschreibung
A.PKI	Die für den Betrieb der Virtuellen Poststelle notwendigen Systemkomponenten der Public-Key-Infrastruktur (PKI) sind vorhanden: • SigG-konforme sichere Signaturerstellungseinheit: – Signaturkarte D-TRUST Card_MS Version 1.0 (Nachtrag zur Bestätigung TUVIT.09361.TE.10.2001 vom 23.10.2001). • SigG-konformer Chipkartenleser: – KOBIL Systems GmbH, KAAN Professional, nur RS232-Version (Bestätigungs-ID: TUVIT.09331.TE.03.2002) – Reiner SCT Kartengeräte GmbH & Co. KG, cyberJack e-com, Version

Annahme	Beschreibung
	2.0, nur USB und Windows (Bestätigungs-ID: TUVIT.09363.TE.06.2002) – Reiner SCT Kartengeräte GmbH & Co. KG, cyberJack pinpad, Version 2.0, nur USB und Windows, (Bestätigungs-ID: TUVIT.09362.TE.05.2002) • qualifizierte Zertifikate und Sicherheitsanker (Trust Anchor); • private Schlüssel (zur Gewährleistung der Systemsicherheit); • Serverzertifikate (zur Gewährleistung der Systemsicherheit). Dabei werden geeignete kryptographische Verfahren mit entsprechenden Schlüssellängen eingesetzt. Eine genaue Beschreibung findet sich im Administrationshandbuch für das Kernsystem und im Administrationshandbuch für das OCSP/CRL-Relay (s. Tabelle 1). Die Serverzertifikate mit den öffentlichen Schlüsseln sowie die geheimen Schlüssel für die elektronischen Signaturen werden durch Schlüsseladministratoren so verteilt, dass eine Kompromittierung ausgeschlossen ist. Zertifikate und Signaturschlüssel werden von einer vertrauenswürdigen Instanz mit Werkzeugen generiert, die denjenigen von akkreditierten Zertifizierungsdiensteanbietern für die entsprechenden Aufgaben entsprechen.
A.SAK	Anfordernde Systeme, die von außen über eine Schnittstelle auf die Basiskomponente zugreifen und deren Funktionalitäten nutzen, stehen zur Verfügung und erfüllen die Anforderungen von Signaturgesetz und –verordnung an eine Signaturanwendungskomponente. Bei der Erzeugung von Batchsignaturen gewährleisten sie insbesondere die folgenden SigG-relevanten Funktionalitäten: • Die Hashwerte über die zu signierenden Daten müssen von dem anfordernden System gebildet werden. • Die vom EVG gelieferten Signaturen müssen durch einen Vergleich mit den ursprünglichen Hashwerten mathematisch verifiziert werden. • Das anfordernde System in der IT-Umgebung muss beim Erzeugen einer Batchsignatur gewährleisten, dass das Auslösen einer Batchsignatur vorher eindeutig angezeigt wird. • Das anfordernde System in der IT-Umgebung muss beim Erzeugen einer Batchsignatur gewährleisten, dass erkennbar ist, auf welche Daten sich die Batchsignatur bezieht. • Bei Bedarf muss ein anforderndes System beim Erzeugen einer Batchsignatur den Inhalt der zu signierenden Daten hinreichend darstellen und somit über eine entsprechende Anzeigeeinheit verfügen. • Das anfordernde System in der IT-Umgebung muss beim Erzeugen einer Batchsignatur gewährleisten, dass die berechtigt signierende Person zuvor erfolgreich identifiziert und authentifiziert wurde. • Ein anforderndes System muss darüber hinaus sicherstellen, dass im Sinne der FAQ 18 der Bundesnetzagentur nur „eine große Anzahl praktisch

Annahme	Beschreibung
	gleicher Vorgänge“[10] der Batchsignatur zugeführt werden. Zur Verifikation von Signaturen müssen anfordernde Systeme insbesondere die folgenden Funktionen bereitstellen: • Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, auf welche Daten sich die Signatur bezieht. • Beim Prüfen einer Signatur muss das anfordernde System gewährleisten, dass erkennbar wird, ob die Daten unverändert sind – also eine geeignete Anzeige bereitstellen. • Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass bei Bedarf der Inhalt der signierten Daten hinreichend zu erkennen ist. • Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist. • Das anfordernde System in der IT-Umgebung muss beim Prüfen einer Signatur gewährleisten, dass erkennbar wird, welche Inhalte das qualifizierte Zertifikat, auf dem die Signatur beruht, und zugehörige qualifizierte Attribut-Zertifikate aufweisen • Sicherheitstechnische Veränderungen müssen erkennbar sein. Anfordernde Systeme und die Basiskomponente müssen sich gemäß den Vorgaben des generischen Sicherheitskonzeptes[11] in einem vertrauenswürdigen Netz befinden. Dies bedeutet insbesondere, dass ein Anschluss der Basiskomponente direkt an das Internet nicht vorhanden sein darf.
A.Betrieb	Für den Betrieb ist vertrauenswürdiges Personal eingesetzt, das einen Beitrag zur Sicherheit leistet, und die notwendigen räumlichen Gegebenheiten sowie Hard- und Software für den sicheren Betrieb (s.u.) sind vorhanden. Dazu gehören auch Signaturschlüssel-Inhaber, die sich beispielsweise vergewissern, dass sie bei der Eingabe ihres Identifikationsmerkmals (PIN) nicht beobachtet werden, oder die ihr Identifikationsmerkmal ändern, wenn sie den Verdacht oder die Gewissheit haben, ihr Merkmal könnte nicht mehr geheim sein. Darüber hinaus sind Administratoren für die verschiedenen Aufgaben benannt, die einen Beitrag zur Sicherstellung einer vertraulichen und integren Betriebsumgebung der Basiskomponente leisten. Die Basiskomponente wird so konfiguriert, dass eine Benutzerkennung entweder einer administrativen Benutzerrolle zugeordnet oder als Signaturschlüssel-Inhaber konfiguriert ist. Es wird gewährleistet, dass die Basiskomponente korrekt aufgebaut ist, inkl. Einhaltung der Vorgaben hinsichtlich der räumlichen Gegebenheiten (dedizierter Raum für die Chipkartenleser) und für die Realisierung der Netzwerkarchitektur und der internen Verbindungen zwischen den einzelnen Systemkomponenten mit Firewall, Demilitarisierter Zone (DMZ) etc. Vgl. dazu die Vorgaben und Auflagen zum Betrieb der Virtuellen Poststelle, die im „Generischen

Annahme	Beschreibung
	Sicherheitskonzept für die Kern- und Webkomponenten der Virtuellen Poststelle“[11] beschrieben werden. Die Anforderungen an einen „geschützten Einsatzbereich (Regelfall/Standardlösung)“ [9] werden umgesetzt, um „potentielle Angriffen über das Internet, ein angeschlossenes Intranet, einen manuellen Zugriff Unbefugter und einen Datenaustausch per Datenträger [...] durch eine Kombination von Sicherheitsvorkehrungen in der Signaturanwendungskomponente selbst und der Einsatzumgebung mit hoher Sicherheit“[9] hinsichtlich eines hohen Angriffspotentials abzuwehren. • Folgende Hardware ist einzusetzen: – 2 GHz i386 (Intel Xeon o.ä) Prozessor mit 2 GB RAM und 40 GB Harddisk oder – Sun Sparc mit 300 MHz-Prozessor mit mindestens 2 GB RAM und 20 GB Harddisk • Eines der folgenden Betriebssysteme muss installiert sein: – Linux (SuSE Linux Enterprise Server 9) – Windows 2003 Server – SUN Solaris 9 • Die folgenden Applikationen sind installiert: – Java: Java 2 Runtime Environment 1.4.2_04 oder dazu kompatible Version. – Application Server: JBoss 3.2.5 inklusive Tomcat 5.0.26 – Datenbank: MySQL 4.1 • Auflagen zur Anbindung an das Internet/Intranet: Es wird angenommen, dass Netzwerkverbindungen so abgesichert sind, dass Angriffe erkannt bzw. unterbunden werden – z. B. durch eine geeignet konfigurierte Firewall. Die Absicherung der Kommunikationsstrecke bei Nutzung von Kernsystem und OCSP/CRL-Relay über ein Weitverkehrsnetz ist geeignet zur Abwehr möglicher Angriffe und geeignete Anti-Viren-Programme bzw. Content-Filter werden verwendet. • Auflagen zur Sicherheit der IT-Plattform und Applikationen: Es wird gewährleistet, dass von der Hardware, auf der die Basiskomponente betrieben wird, keine Angriffe ausgehen. Insbesondere ist sicherzustellen, dass die auf dem eingesetzten Computer installierte Software nicht böswillig manipuliert oder verändert werden kann, auf dem Computer keine Viren oder Trojanischen Pferde eingespielt werden können, die Hardware des Computers nicht unzulässig verändert werden kann, der verwendete Chipkartenleser nicht böswillig manipuliert wurde,

[11] BundOnline 2005, Bundesamt für Sicherheit in der Informationstechnik, bremen online services GmbH & Co. KG, datenschutz nord GmbH, „Generisches Sicherheitskonzept für dieKern- und Webkomponenten der Virtuellen Poststelle“, 2004. Siehe auch die E-Government-Seite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter www.bsi.bund.de/fachthem/vps/index.htm.

Annahme	Beschreibung
	um Daten (z. B. PIN, Hashwerte etc.) auszuforschen oder zu verändern (laut der einheitlichen Spezifizierung der Einsatzbedingungen[9], Fußnote 26: „IT-Plattform und die Applikationen müssen so vertrauenswürdig sein, dass die Sicherheitsfunktionen [...] mit hoher Sicherheit nicht beeinträchtigt werden. Sie müssen dazu insbesondere frei von Schadensprogrammen (Computerviren, trojanischen Pferde usw.) sein.“). • Auflagen zum Schutz vor manuellem Zugriff Unbefugter und Datenaustausch per Datenträger: Es wird angenommen, dass die folgenden baulichen, personellen und organisatorischen Anforderungen umgesetzt sind: • Die "Signatur-Arbeitstation"[9], bestehend aus der Basiskomponente, Chipkartenleser, Signaturkarten, Monitor, Tastatur und Rechner befindet sich in einem zugriffssicheren Betriebsraum, so dass gemäß der einheitlichen Spezifizierung der Einsatzbedingungen[9], Fußnote 10 „ein Zugriff Unbefugter ausgeschlossen ist oder zumindest mit hoher Sicherheit erkennbar wird“. • Rechner und Chipkartenleser sind durch einen sicheren Kanal, d.h. direkt durch ein Kabel, verbunden. • Für die Administratoren müssen Vertreterregelungen für Krankheit und Urlaub bestehen. • Wartungs- bzw. Reinigungspersonal erhalten den Zugang zum zugriffssicheren Betriebsraum nur durch einen System-Administrator, der den Aufenthalt überwacht. • Ein Signaturschlüssel-Inhaber erhält den Zugang zum zugriffssicheren Betriebsraum nur durch den Schlüssel-Administrator, der den Aufenthalt überwacht. • Ein Security-Administrator wird durch einen Revisor überwacht. • Ein Schlüssel-Administrator wird von einem System-Administrator begleitet.
A.Dir	Ein SigG-konformer Verzeichnisdienst für Sperrlisten und Zertifikatsstatusabfragen zur Validierung von qualifizierten Zertifikaten ist vorhanden und es besteht eine Verbindung dorthin.
A.ZufPIN	Die Einsatzumgebung mit SigG-konformem Chipkartenleser (mit PIN-Pad) und Signaturkarte gewährleistet, dass die Identifikationsdaten nicht preisgegeben und nur auf der jeweiligen sicheren Signaturerstellungseinheit gespeichert werden. Daher dürfen nur die in der Annahme A.PKI genannten bestätigten sicheren Signaturerstellungseinheiten und bestätigten Kartenleser eingesetzt werden.

Tabelle 3: Einsatzbedingungen für die Basiskomponente

3.3 Algorithmen und zugehörige Parameter

Die verwendeten kryptografischen Algorithmen sind gemäß der Veröffentlichung der Bundesnetzagentur[12] als geeignet eingestuft.

Zur Absicherung der Kommunikation zwischen der Basiskomponente und externen Systemen werden elektronische Signaturen eingesetzt, die auf dem RSA-Verfahren mit einer Schlüssellänge von 2048 Bit und dem Hashalgorithmus SHA-1 basieren.

Zur Prüfung qualifizierter elektronischer Signaturen werden von der Basiskomponente die Hashfunktion SHA-1 sowie der RSA-Algorithmus mit einer Schlüssellänge von mindestens 1024 Bit bereitgestellt.

Der verwendete Hashalgorithmus SHA-1 gilt derzeit bis **Ende 2009** als geeignet.

Der RSA-Algorithmus mit einer Schlüssellänge von 1024 Bit gilt bis **Ende 2007** als geeignet. Für die Gewährleistung eines langfristigen Sicherheitsniveaus wird grundsätzlich die Erhöhung auf 2048 Bit empfohlen.

3.4 Prüfstufe und Mechanismenstärke

Das Produkt „Virtuelle Poststelle des Bundes Version 2.2.2.6 (Basis)“ wurde erfolgreich nach den Common Criteria (CC) mit der Prüfstufe **EAL3+** (EAL3 mit Zusatz[13] AVA_VLA.4 (gegen ein hohes Angriffspotential), AVA_MSU.3 (eine vollständige Missbrauchsanalyse), ADV_IMP.1, ADV_LLD.1 und ALC_TAT.1, ADO_DEL.2 (Erkennung von Manipulation)) evaluiert.

Die eingesetzten Sicherheitsfunktionen erreichen die Stärke **hoch**.

Ende der Bestätigung

[12] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 22. Februar 2007, veröffentlicht am 12. April 2007 im Bundesanzeiger Nr. 69, S. 3759

[13] Gemäß § 11 Abs. 3 in Verbindung mit Anlage 1 Abschnitt I Nr. 1 SigV.